PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 17 October 2000 (17.10.00)	
International application No. PCT/GB00/00370	**Applicant's or agent's file reference** 30990020 WO
International filing date (day/month/year) 08 February 2000 (08.02.00)	**Priority date** (day/month/year) 08 February 1999 (08.02.99)
Applicant MAO, Wenbo	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

04 September 2000 (04.09.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Pascal Piriou

Telephone No.: (41-22) 338.83.38

EL652176636US

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application No.

International Filing Date

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* 30990020 WO

Box No. I TITLE OF INVENTION

Verification of the Private Components of a Public-Key Cryptographic System

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304
US

☐ This person is also inventor.

Telephone No.

Facsimile No.

Teleprinter No.

State *(that is, country)* of nationality: US

State *(that is, country)* of residence: US

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

MAO, Wenbo
60 Wheatfield Drive
Bradley Stoke
Bristol BS32 9DD
GB

This person is:

☐ applicant only

☒ applicant and inventor

☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: CN

State *(that is, country)* of residence: GB

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

LAWRENCE, Richard Anthony
Hewlett-Packard Limited
Intellectual Property Section
Filton Road
Stoke Gifford, Bristol BS34 8QZ
GB

Telephone No. (0)117-312-8295

Facsimile No. (0)117-312-8941

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

☐ **AP** **ARIPO Patent:** **GH** Ghana, **GM** Gambia, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **SD** Sudan, **SL** Sierra Leone, **SZ** Swaziland, **TZ** United Republic of Tanzania, **UG** Uganda, **ZW** Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT

☐ **EA** **Eurasian Patent:** **AM** Armenia, **AZ** Azerbaijan, **BY** Belarus, **KG** Kyrgyzstan, **KZ** Kazakhstan, **MD** Republic of Moldova, **RU** Russian Federation, **TJ** Tajikistan, **TM** Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

☒ **EP** **European Patent:** **AT** Austria, **BE** Belgium, **CH and LI** Switzerland and Liechtenstein, **CY** Cyprus, **DE** Germany, **DK** Denmark, **ES** Spain, **FI** Finland, **FR** France, **GB** United Kingdom, **GR** Greece, **IE** Ireland, **IT** Italy, **LU** Luxembourg, **MC** Monaco, **NL** Netherlands, **PT** Portugal, **SE** Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☐ **OA** **OAPI Patent:** **BF** Burkina Faso, **BJ** Benin, **CF** Central African Republic, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroon, **GA** Gabon, **GN** Guinea, **GW** Guinea-Bissau, **ML** Mali, **MR** Mauritania, **NE** Niger, **SN** Senegal, **TD** Chad, **TG** Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* .....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

☐ **AE** United Arab Emirates
☐ **AL** Albania
☐ **AM** Armenia
☐ **AT** Austria
☒ **AU** Australia
☐ **AZ** Azerbaijan
☐ **BA** Bosnia and Herzegovina
☐ **BB** Barbados
☐ **BG** Bulgaria
☐ **BR** Brazil
☐ **BY** Belarus
☐ **CA** Canada
☐ **CH and LI** Switzerland and Liechtenstein
☐ **CN** China
☐ **CR** Costa Rica
☐ **CU** Cuba
☐ **CZ** Czech Republic
☐ **DE** Germany
☐ **DK** Denmark
☐ **DM** Dominica
☐ **EE** Estonia
☐ **ES** Spain
☐ **FI** Finland
☐ **GB** United Kingdom
☐ **GD** Grenada
☐ **GE** Georgia
☐ **GH** Ghana
☐ **GM** Gambia
☐ **HR** Croatia
☐ **HU** Hungary
☐ **ID** Indonesia
☐ **IL** Israel
☐ **IN** India
☐ **IS** Iceland
☐ **JP** Japan
☐ **KE** Kenya
☐ **KG** Kyrgyzstan
☐ **KP** Democratic People's Republic of Korea
☐ **KR** Republic of Korea
☐ **KZ** Kazakhstan
☐ **LC** Saint Lucia
☐ **LK** Sri Lanka
☐ **LR** Liberia
☐ **LS** Lesotho
☐ **LT** Lithuania
☐ **LU** Luxembourg
☐ **LV** Latvia
☐ **MA** Morocco
☐ **MD** Republic of Moldova
☐ **MG** Madagascar
☐ **MK** The former Yugoslav Republic of Macedonia
☐ **MN** Mongolia
☐ **MW** Malawi
☐ **MX** Mexico
☐ **NO** Norway
☐ **NZ** New Zealand
☐ **PL** Poland
☐ **PT** Portugal
☐ **RO** Romania
☐ **RU** Russian Federation
☐ **SD** Sudan
☐ **SE** Sweden
☐ **SG** Singapore
☐ **SI** Slovenia
☐ **SK** Slovakia
☐ **SL** Sierra Leone
☐ **TJ** Tajikistan
☐ **TM** Turkmenistan
☐ **TR** Turkey
☐ **TT** Trinidad and Tobago
☐ **TZ** United Republic of Tanzania
☐ **UA** Ukraine
☐ **UG** Uganda
☒ **US** United States of America
☐ **UZ** Uzbekistan
☐ **VN** Viet Nam
☐ **YU** Yugoslavia
☐ **ZA** South Africa
☐ **ZW** Zimbabwe

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

☐ .....
☐ .....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) (08/02/99) 8 February 1999	9902687.4	GB		
item (2)				
item (3)				

☐ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s):

* *Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)* : ISA /

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*:

Date (day/month/year)	Number	Country (or regional Office)
24 August 1999	9902687.4	GB

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets**:

request	: 3
description (excluding sequence listing part)	: 29
claims	: 5
abstract	: 1
drawings	: 9
sequence listing part of description	:
Total number of sheets	: 47

This international application is **accompanied** by the item(s) marked below:

1. ☒ fee calculation sheet
2. ☒ separate signed power of attorney
3. ☒ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☒ priority document(s) identified in Box No. VI as item(s): 1
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☒ other *(specify)*: Search Report

Figure of the drawings which should accompany the abstract: 3

Language of filing of the international application: English

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Richard Anthony Lawrence

For receiving Office use only

1. Date of actual receipt of the purported international application:	2. Drawings: ☐ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:	
4. Date of timely receipt of the required corrections under PCT Article 11(2):	
5. International Searching Authority (if two or more are competent): ISA /	6. ☐ Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

L652176636US

The demand must be filed directly with the competent International Preliminary Examining Authority or, if two or more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ EP

PCT

CHAPTER II

DEMAND

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only

Identification of IPEA	Date of receipt of DEMAND

Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION		Applicant's or agent's file reference: 30990020 WO
International application No.: PCT/GB00/00370	International filing date *(day/month/year)*: 8 February 2000 (08/02/00)	(Earliest) Priority date *(day/month/year)*: 8 February 1999 (08/02/99)

Title of invention: Verification of the private components of a public-key cryptographic system

Box No. II APPLICANT(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304
US

Telephone No.:

Facsimile No.:

Teleprinter No.:

State *(that is, country)* of nationality: US

State *(that is, country)* of residence: US

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

MAO, Wenbo
60 Wheatfield Drive
Bradley Stoke
Bristol BS32 9DD
GB

State *(that is, country)* of nationality: CN

State *(that is, country)* of residence: GB

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

☐ Further applicants are indicated on a continuation sheet.

International application No.
PCT/GB00/00370

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The following person is ☒ agent ☐ common representative

and ☒ has been appointed earlier and represents the applicant(s) also for international preliminary examination.

☐ is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.

☐ is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

LAWRENCE, Richard Anthony
Hewlett-Packard Limited
Intellectual Property Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ
GB

Telephone No.: (0)117-312-8295

Facsimile No.: (0)117-312-8941

Teleprinter No.:

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION

Statement concerning amendments:*

1. The applicant wishes the international preliminary examination **to start on the basis of:**

☒ the international application as originally filed

the description ☐ as originally filed
☐ as amended under Article 34

the claims ☐ as originally filed
☐ as amended under Article 19 (together with any accompanying statement)
☐ as amended under Article 34

the drawings ☐ as originally filed
☐ as amended under Article 34

2. ☐ The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.

3. ☐ The applicant wishes the start of the international preliminary examination **to be postponed** until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English

☒ which is the language in which the international application was filed.
☐ which is the language of a translation furnished for the purposes of international search.
☐ which is the language of publication of the international application.
☐ which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

Box No. V ELECTION OF STATES

The applicant hereby **elects all eligible States** *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes **not to elect:**

International application No.
PCT/GB00/00370

Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:			For International Preliminary Examining Authority use only: received	not received
1. translation of international application	:	sheets	☐	☐
2. amendments under Article 34	:	sheets	☐	☐
3. copy (or, where required, translation) of amendments under Article 19	:	sheets	☐	☐
4. copy (or, where required, translation) of statement under Article 19	:	sheets	☐	☐
5. letter	:	sheets	☐	☐
6. other *(specify)*	:	sheets	☐	☐

The demand is also accompanied by the item(s) marked below:

1. ☒ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ nucleotide and or amino acid sequence listing in computer readable form
6. ☐ other *(specify)*:

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).

Richard Anthony Lawrence

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:
2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
3. ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. ☐ The applicant has been informed accordingly.
4. ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.
5. ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
30990020 WO		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB00/00370	08/02/2000	08/02/1999
International Patent Classification (IPC) or national classification and IPC H04L9/32		
Applicant HEWLETT-PACKARD COMPANY et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 1 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
04/09/2000	14.03.2001
Name and mailing address of the international preliminary examining authority: European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Authorized officer Zucka, G Telephone No. +31 70 340 4026

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB00/00370

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

1-29	as originally filed				

Claims, No.:

1-6,7 (part)	as originally filed				
7 (part),8-13	as received on	13/01/2001	with letter of	05/01/2001	

Drawings, sheets:

1/9-9/9	as originally filed				

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-13
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-13
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-13
	No:	Claims	

2. Citations and explanations
   see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Ad V:

1. Reference is made to the following document:

   D1: R. BERGER, S. KANNAN, R. PERALTA: 'A Framework for the Study of Cryptographic Protocols' ADVANCES IN CRYPTOLOGY - PROCEEDINGS OF CRYPTO 85, 18 - 22 August 1985, pages 87-103, XP002136911 cited in the application

2. The document D1 (cited on page 2 of the description) discloses a method of exchanging public key verification data, which just like the method of the independent claim 1, uses a zero-knowledge proof.

3. The method of claim 1 distinguishes itself from the prior art, in that a Monte-Carlo test for primality is carried out in a specific way.

   The method has the advantage of proving the two-prime product structure of a number with a cost of $O(k\log_2 n)$ multiplications and an error probability of $1/2^k$ (if $k = 60$, $n > 2^{512}$, and $1/2^k >> 24/n^{1/4}$), regardless of whether the number in question is a Blum integer or not.

   Such a way of proceeding is not disclosed or rendered obvious by any of the documents cited in the search report, and the subject-matter of claim 1 is therefore both new and inventive.

4. The independent claims 4 and 7 relate to devices carrying out the method of claim 1, and the independent claim 13 relates to a computer storage medium containing a corresponding program. The subject-matter of these claims is consequently new and inventive for the same reasons as indicated above.

5. Claims 2-3, 5-6, and 8-12 are truly dependent claims, and their subject-matter is therefore also new and inventive.

6. The subject-matter of claims 1-13 is industrially applicable.

Ad VIII:

Some of the claims contain expressions between brackets which are not reference signs, but instead are intended to be part of the definition for the claimed subject-matter, e.g. the expression "(I(p),I(q))" in claim 1. This renders the claims unclear (Article 6 PCT).

The expressions would have been considered clear without the enclosing brackets.

e) check that $\left(\frac{h}{n}\right) = -1$ and, if so, select two random numbers u and v such that $\ell(u) = \ell((p-1)/2)$, $\ell(v) = \ell((q-1)/2)$ and provide to said other computing entity the values $U = g^u$, $V = g^v$, $H_U = B^{(h^u \bmod n)}$, $H_V = A^{(h^v \bmod n)}$ and $H_{UV} = h^u h^v \bmod n$;

f) receive from said other computing entity a request to provide to said other computing entity values r and s, which said other computing entity randomly specifies should be either:

(1) $r = u$ and $s = v$, or

(2) $r = u + (p-1)/2$, $s = v + (q-1)/2$

g) provide the requested values r and s to said other computing entity.

8. A method as claimed in claim 7 in which $d \leq 2$.

9. A method as claimed in claim 7 in which at least one of the selections of random numbers uniformly distributed.

10. A system of co-operating computer entities including a first computing entity as claimed in claim 4 and a second computing entity as claimed in claim 7.

11. A communication system comprising at least a pair of computing entities as claimed in claim 10 and a communications medium, each of said pair of computing entities being arranged to communicate with the other computing entity via the communications medium.

12. A communication system as claimed in claim 11 in which said communications medium includes one or more of any of the internet, local area network, wide area network, virtual private circuit or public telecommunications network.

13. A computer storage medium having stored thereon a computer program readable by a general purpose computer, the computer program including instructions for said general purpose computer to configure it to be as said computer entity as claimed in claim 4 or said computer entity as claimed in claim 7.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/32, 9/30

A1

(11) International Publication Number: WO 00/48359

(43) International Publication Date: 17 August 2000 (17.08.00)

(21) International Application Number: PCT/GB00/00370

(22) International Filing Date: 8 February 2000 (08.02.00)

(30) Priority Data:
9902687.4 8 February 1999 (08.02.99) GB

(71) Applicant *(for all designated States except US)*: HEWLETT-PACKARD COMPANY [US/US]; 3000 Hanover Street, Palo Alto, CA 94304 (US).

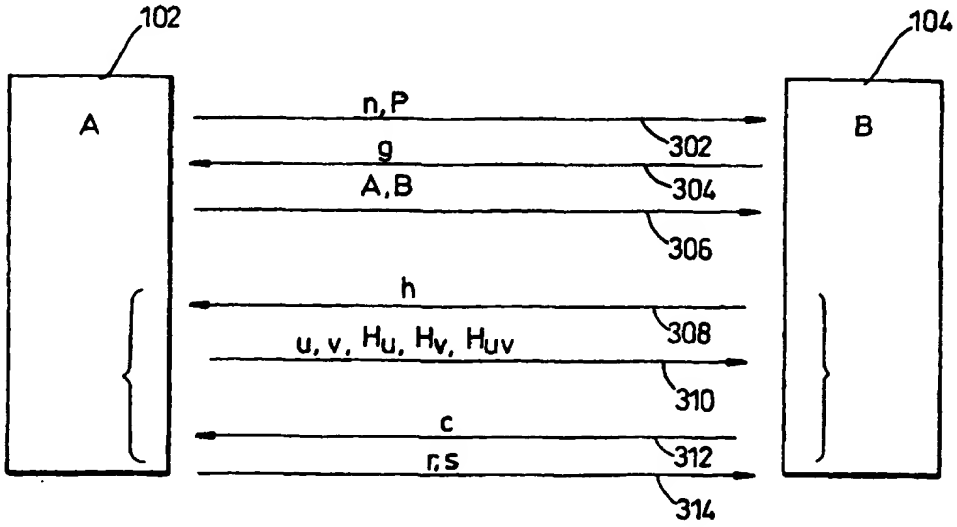
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: MAO, Wenbo [CN/GB]; 60 Wheatfield Drive, Bradley Stoke, Bristol BS32 9DD (GB).

(74) Agent: LAWRENCE, Richard, Anthony; Hewlett-Packard Limited, Intellectual Property Section, Filton Road, Stoke Gifford, Bristol BS34 8QZ (GB).

(81) Designated States: AU, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: VERIFICATION OF THE PRIVATE COMPONENTS OF A PUBLIC-KEY CRYPTOGRAPHIC SYSTEM



(57) Abstract

A method of exchanging digital public-key verification data whereby a first computing entity (102) enables a second computing entity (104) to obtain probabilistic evidence that a given public-key number n is the product of exactly two odd primes p and q, not known to the second party, whose bit lengths ($l(p)$, $l(q)$ differ by not more than d bits. The method provides an efficient proof of knowledge protocol for demonstrating Monte-Carlo evidence that a number n is the product of two odd primes of roughly equal size. The evidence is shown "in the dark", which means that the structure is verified without the prime factors of n disclosed. The cost of a proof amounts to $12k\log_2 n$ multiplications of integers of size of n where k is the number of the iterations in the proof and relates to an error probability bounded by $\max(1/2^k, 24/n^{1/4})$.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Verification of the private components of a public-key cryptographic system

Technical field

This invention relates to apparatus and methods for verifying the private components of a public-key cryptographic system.

Background to the invention

Electronic commerce plays an increasingly important role in modern society and necessarily involves the transmission of electronic data between two parties. In a commercial environment, a first party may wish to transmit electronic data to a second party over an intervening communications network, in particular the internet, only when confident that there is adequate security against eavesdroppers that may be present on the network. The parties may be computer entities, for example.

One way to achieve this is for the first party to encrypt the data in a manner that only the second party can decrypt after receipt. One class of such encryption techniques, and with which the present invention is concerned, is public-key cryptography based on the computational difficulty of factoring large integers. The first party encrypts a message by use of a public-key published by the second party the crypted message only being practicably decrypted by use of corresponding private components of the key held by the second party. These techniques include the well-known RSA cryptosystem, for example.

In many cases, the first party will not wish to use the encryption system without being confident that the public-key to be used to encrypt the data conforms to an agreed set of criteria related to the security of the encryption to be obtained. One way to achieve this is to seek a certificate from a trusted certification authority that has verified to its own satisfaction that the public-key does so conform. An alternative way is for the first party to seek verification directly from the second party. Whatever the route to verification, the owner of the public-key generally prefers, and it is often a requirement of the encryption standard adopted, that the proof that the public-key is as it is claimed is achieved without revealing the private component to the verifier. That is, the proving party runs what is called a protocol with the verifying party that provides a 'knowledge proof' of the validity

of the private components. For instance, the ISO standardization document 9798 part 3 recommends that public-key certification include knowledge proof for possession of the private component that matches the pubic key to be certified.

An example of such a set of criteria known to provide a highly secure public-key is that the public-key is an integer (n) which is the product of only two odd primes (p,q) and that the primes have lengths in bits which differ by no more than a predetermined value, d, commonly equal to 2.

Given the computational intractability of factoring large integers, there exists no known algorithm that can be input a given number n and terminate in a polynomial time in the size of n with an output answering whether n is the product of exactly two odd primes. Nevertheless, there do exist practically efficient interactive protocols that run in polynomial time and allow a prover who knows the factorization of n to prove such a structure to the satisfaction of a verifier without disclosing the factorization information to the latter.

An early idea for proving n in such a structure is based on an observation due to Adleman [see R. Berger, S. Kannan and R. Peralta. A framework for the study of cryptographic protocols, Advances in Cryptology – Proceedings of CRYPTO 85 (H.C. Williams ed.), Lecture Notes in Computer Science, Springer-Verlag 218 (1986), pp. 87-103]. He suggested using the fact that if n has exactly two different prime factors (which may include their powers) then exactly a quarter of the elements in the multiplicative group mod n are quadratic residues (square numbers of n). On the other hand, if n has more than two prime factors then at most one-eighth of them are quadratic residues. Thus a prover, knowing the factorization of n, can show a verifier the structure via binomial trials that for a set of k elements randomly chosen from the multiplicative group mod n, roughly $k/4$ of them are quadratic residues (shown by disclosing to the verifier their square roots). Using a normal distribution as an approximation to the probability of binomial trials (a standard method), Berger et al [R. Berger, S. Kannan and R. Peralta. A framework for the study of cryptographic protocols, Advances in Cryptology – Proceedings of CRYPTO 85 (H.C. Williams ed.), Lecture Notes in Computer Science, Springer-Verlag 218 (1986), pp. 87-103] established that if $\frac{\sqrt{21}-1}{20}k$ or more such elements are shown to be quadratic residues then the proof should be accepted with the probability of error between $e^{-k/74}$ and $e^{-k/75}$.

Thus, k should be in thousands ($k = 3000$ was suggested in [R. Berger, S. Kannan and R. Peralta. A framework for the study of cryptographic protocols, Advances in Cryptology – Proceedings of CRYPTO 85 (H.C. Williams ed.), Lecture Notes in Computer Science, Springer-Verlag 218 (1986), pp. 87-103]) in order for the error probability to be negligibly small. (We note $e^{-3000/74} < 1/2^{58} < e^{-3000/75}$ and regard an amount at this level to be negligibly small). Since the cost for computing a square root mod n is measured by $O(\log_2 n)$ multiplications of integers mod n, the total cost for proving the two-prime-product structure of a number n by showing quadratic residue information will be $O(k\log_2 n)$ (multiplications mod n) with an error probability between $e^{-k/74}$ and $e^{-k/75}$.

Van de Graaf and Peralta [J. van de Graaf and R. Peralta. A simple and secure way to show the validity of your public-key, Advances in Cryptology – Proceedings of CRYPTO 87 (E. Pomerance, ed.), Lecture Notes in Computer Science, Springer-Verlag 293 (1988), pp. 128-134] observed that if n is a Blum integer, that is, n is the product of two distinct prime factors (again this may include their powers), both congruent to 3 mod 4, then any element in the multiplicative group mod n with the positive Jacobi symbol has the property that either itself or its negation is a quadratic residue modulo n. Their protocol for proof of Blum integer is based on this fact. A number of other previous protocols for proving two-prime-product structure also use this idea (e.g., [J. Camenisch and M. Michels. Proving in zero-knowledge that a number is the product of two safe primes, In Advances in Cryptology – EUROCRYPT 99, Lecture Notes in Computer Science, Springer-Verlag 1592 (1999), pp. 106-121, R. Gennaro, D. Miccianicio and T. Rabin.. An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products, In 5th ACM Conference on Computer and Communications Security, October 1998, M. Liskov and R.D. Silverman. A statistical limited-knowledge proof for secure RSA keys, IEEE P1363 Research Contributions, Available at `http://grouper.ieee.org/groups/1363/contributions/ifkeyval.ps`]). Note that provided n is not a square number (which is easy to test against), exactly half of the elements in the multiplicative group mod n can have a positive Jacobi symbol which is also easy to evaluate. Thus, given such n, the above demonstration actually shows that a quarter of elements in the group are quadratic residues (since a quadratic residue must have positive Legendre symbol mod all prime factors, and only half of elements mod a prime

have positive Jacobi symbol). If n is not in a two-prime-product structure then it is certainly not a Blum integer. Omitting details, for any group element of positive Jacobi symbol mod such n (which is non-Blum and non-square), a prover will have at most a 50% chance of correctly demonstrating the above. Clearly, such a proof using k random challenges will result in an error probability bounded by $1/2^k$, which approaches zero much faster than $e^{-k/4}$. (See the comparison between them in the previous paragraph).

The simplest way to show quadratic residue evidence to display a square root of a quadratic residue. In the protocol of Van de Graaf and Peralta for proving Blum integer, the verifier should check that the Jacobi symbol of a square root of a random challenge comply with a pre-agreed random sign. This follows Blum's observation that if n is a Blum integer, then any quadratic residue has square roots of positive and negative Jacobi symbols [M. Blum. Coin flipping by telephone: a protocol for solving impossible problems, Proceedings of *24th IEEE Computer Conference (CompCon(*, 1982, pp. 133-137.]. In the protocol of Gennaro et al [R. Gennaro, D. Miccianicio and T. Rabin. An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products, In 5th ACM Conference on Computer and Communications Security, October 1998.], a verifier should require that for each challenge g sent as challenge, a square root of either $\pm g$ or $\pm 2g$ mod n will be replied. It is possible for a prover to correctly respond to such challenges if one of the prime factors of n is congruent to 5 mod 8, and the other to 7 mod 8. These form an additional constraint to n being a Blum integer.

Note that two different square roots of a quadratic residue mod n can lead to factoring n with a non-trivial probability. So it will be dangerous for a prover to disclose a square root of a challenge which is solely selected by the verifier. The two protocols in R. Gennaro, D. Miccianicio and T. Rabin. An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products, In 5th ACM Conference on Computer and Communications Security, October 1998 J. van de Graaf and R. Peralta. A simple and secure way to show the validity of your public-key, Advances in Cryptology - Proceedings of CRYPTO 87 (E. Pomerance, ed.), Lecture Notes in Computer Science, Springer-Verlag 293 (1988), pp. 128-134 assume the existence of mutually trusted random source which is accessible be the prover and verifier. The applicant believes that it will be costly to implement a mutually trusted random source between two mutually untrusted

parties. The cost can be estimated by a protocol that allows the two parties to generate mutually trusted random elements without using a trusted third party. Blum's idea of coin flipping [M. Blum. Coin flipping by telephone: a protocol for solving impossible problems, Proceedings of *24th IEEE Computer Conference (CompCon)*, 1982, pp. 133-137.] is such a protocol and is used by R. Berger, S. Kannan and R. Peralta. [A framework for the study of cryptographic protocols, Advances in Cryptology – Proceedings of CRYPTO 85 (H.C. Williams ed.), Lecture Notes in Computer Science, Springer-Verlag 218 (1986), pp. 87-103, Z. Galil, S. Haber and M. Yung. A private interactive test of a boolean predicate and minimum-knowledge public-key cryptosystems, *26th FOCS*, 1985, pp. 360-371]. Each instantiation of that protocol generates a truly random bit. Each random challenge of size of n generated this way takes $\log_2 n$ iterations and the same number of multi-precision operations of integers mod n (evaluation of $\log_2 n$ Jacobi symbols). Together $k \log_2 n$ iterations are needed for merely agreeing on k mutually trusted random challenges.

Above we have analyzed the cost for the previous protocols to prove an integer in the two-prime-power structure, i.e., $n = p^r s^s$ where p, q are distinct primes and r, s, integers. To further prove $r = s = 1$ one can use the protocol of Boyar et al [J. Boyar, K. Friedl and C. Lund. Practical zero-knowledge proofs: Giving hints and using deficiencies, Advances in Cryptology – Proceedings of EUROCRYPT 89 (J.-j. Quisquater and J. Vandewalle, eds.), Lecture Notes in Computer Science, Springer-Verlag 434 (1990), pp. 155-172.] for proving square-free integers. Furthermore, to show that p and q are roughly equal size one can use Damgard's method of "checking commitment" protocol [I.B. Damgard. Practical and provably secure release of a secret and exchange of signatures, Advances in Cryptology: Proceedings of EUROCRYPT 93 (T. Helleseth, ed.), Lecture Notes in Computer Science, Springer-Verlag, 765 (1994), pp. 201-217.]. However, the costs of applying these two additional protocols will be ignored because they are less expensive than that for proving the two-prime-power structure, in particular for the case of non-Blum integers.

Solovay and Strassen disclosed, in an article titled "A Fast Monte-Carlo Test for Primality" SIAM J. COMPUTING Vol 6, No 1, March 1977, an efficient Monte-Carlo test for determining the probability that a given odd integer n is prime. The probability that n is

composite is $< 1/2^k$ if $a^{(x-1)/2} \equiv \left(\frac{a}{x}\right) (\mathrm{mod}\, x)$ for all of k random values of $a<x$, where $\left(\frac{a}{x}\right)$ is the Jacobi symbol of a mod x.

This "Solovay-Strassen" test can provide an efficient means for determining the probability that each of p and q are primes, where $n = p.q$, by submitting p and q to the test in turn. However, this requires p and q to be disclosed to the person verifying that n is product of two, only, primes.

To better understand the operation of the methods disclosed herein, the following terminology is used.

Let P be a positive integer. Z_P^* denotes the multiplicative group of elements mod P. For $a \in Z_P^*$, $Ord_P(a)$ denote the order of a mod P.

Let a and b be integers. $a|b$ denotes a dividing b; (a, b) denotes the greatest common divisor of a and b; $\left(\frac{a}{b}\right)$ denotes the Jacobi symbol of a mod b; $\ell(a)$ denotes the size of a, which is the number of the bits in the binary representation of a.

Let x be a real number. $\lfloor x \rfloor$ denotes the integer part of x (thus $\ell(a) = \lfloor \log_2(a) \rfloor + 1$); $|x|$ denotes the absolute value of x.

Let S be a set. $\#S$ denotes the cardinality of S.

Finally, $Pr[E]$ denotes the probability for event E to occur.

The present applicant has determined that a Monte-Carlo test of the primality of a both of positive integers p and q, where $n = p.q$ can comprise the following steps:

a) find a prime number P such that $n|(P-1)$;

b) select any positive integer f such that $A \neq B, A \neq 1, B \neq 1$ where

$$A = g^p \mathrm{mod} P,$$

$$B = g^q \mathrm{mod} P, \text{ and}$$

$$g = f^{(P-1)/n} \mathrm{mod} P;$$

then repeatedly:

c) choose a random $h \in Z_n^*$ and $\left(\frac{h}{n}\right) = -1$;

d) choose random positive integers u, v;

e) calculate, mod$P$;

$$H_U = B^{(h^u \bmod n)};$$

$$H_V = A^{(h^v \bmod n)};$$

$r = u + (p - 1)/2;$

$s = v + (q - 1)/2;$

f) determine whether, mod$P$,

$$B^{(h^r \bmod n)} = H_U^{\pm 1} \text{ ;and}$$

$$A^{(h^s \bmod n)} = H_U^{\mp 1}.$$

It can be seen that the results of a Solovay-Strassen primality test are obtained on both p and q by steps f) of this method. Furthermore, the applicant has determined that the difficulty of finding p and q from knowledge of n, A and B of this test is at least as difficult as solving the decision problem on the membership of the Diffe-Hellman quadruples generated by g. (This is assumes that factorization of n and computing discrete logarithms to the base g are infeasible). Thus, if a verifier could be convinced that a prover has provided values for step f) which are properly related to p, q and the value of h (supplied by the verifier), the verifier would equally be confident of the Solovay-Strassen primality test using those values provide.

The present invention is as claimed in the claims.

Summary of the invention

The present invention, in a first aspect, provides a method of exchanging digital public-key verification data whereby a first party enables a second party to obtain probabilistic evidence that a given public-key number n is the product of exactly two odd primes p and q, not known to the second party, whose bit lengths ($\ell(p)$, $\ell(q)$) differ by not more than d bits. The method including the following steps, all operations being to mod P

unless specified mod n, the method being halted should any check fail. Initial parameters are established by:

a) said first party provides to said second party a number P such that P is a prime number and $n|(P-1)$;

b) said second party provides to said first party a number g where

$g = f^{(P-1)/n} \bmod P$, $f < P$;

c) said first party provides to said second party numbers A and B, where

$A = g^p \bmod P$ and $B = g^q \bmod P$.

Thereafter:

d) said second party checks that $A \neq B, A \neq 1$ and $B \neq 1$; whereupon the following steps are repeated up to k times;

e) said second party selects a random number $h \in Z_n^*$ such that $\left(\frac{h}{n}\right) = -1$ and provides the number h to the first party;

f) said first party checks that $\left(\frac{h}{n}\right) = -1$ and selects two random numbers u and v such that $\ell(u) = \ell((p-1)/2)$, $\ell(v) = \ell((q-1)/2)$ and provides to said second party the values $U = g^{2u}$, $V = g^{2v}$, $H_U = B^{\left(h^u \bmod n\right)}$,

g) $H_V = A^{\left(h^v \bmod n\right)}$, and $H_{UV} = h^u h^v \bmod n$;

g) said second party sends a request to the first party that the first party provides to the second party values r and s, which the second party randomly specifies should be either:

(1) $r = u$ and $s = v$; or

(2) $r = u + (p-1)/2$, $s = v + (q-1)/2$

h) said first party provides the requested values r and s to the second party,

i) if the second party requested $r = u$ and $s = v$, the second party determines whether:

(1) $\ell(r) \leq \lfloor \ell(n)/2 \rfloor + d$, $\ell(s) \leq \lfloor \ell(n)/2 \rfloor + d$,

(2) $g^{2r+1} \equiv Ug$, $g^{2s+1} \equiv Vg$,

(3) $B^{(h^r \bmod n)} \equiv H_U, \quad A^{(h^s \bmod n)} \equiv H_V$, and

(4) $h^r h^s \equiv H_{UV} \pmod n$;

thereby verifying the values provided by the first party to the second party are as were required by steps a) to f); or, if the second party requested $r = u + (p - 1)/2$, $s = v + (q - 1)/2$,

the second party determines whether:

(1) $\ell(r) \le \lfloor \ell(n)/2 \rfloor + d, \quad \ell(s) \le \lfloor \ell(n)/2 \rfloor + d$,

(2) $g^{2r+1} \equiv UA, \quad g^{2s+1} \equiv VB$,

(3) $B^{(h^r \bmod n)} \equiv H_U^{\pm 1}, \quad A^{(h^s \bmod n)} \equiv H_V^{\mp 1}$

($\pm$ *and* $\mp$ meaning the two exponents are of opposite sign), and

(4) $h^r h^s \equiv H_{UV} h^{(n-1)/2} \pmod n$,

thereby obtaining said probabilistic evidence on whether the given public-key number n is the product of exactly two odd primes p and q whose bit lengths ($\ell(p)$, $\ell(q)$) differ by not more than d bits.

The cost of a proof amounts to $12k\log_2 n$ multiplications of integers of size of n where k is the number of the iterations in the proof and relates to an error probability bounded by $\max(1/2^k, 24/n^{1/4})$. To achieve cost and error similar to these, previous techniques require two additional conditions: (1) n is a Blum integer, and (2) a mutually trusted $k\log_2 n$-bit long random source is accessible by the proving/verification participants. In failure of (1), k must be increased substantially in order to keep error probability comparably small (e.g., k should be increased to 3000 for an error probability to remain at the level of $\frac{1}{2}^{60}$).

The present invention, in further aspects, encompasses computing entities and a communications system, a system of co-operating computing entities all for carrying out this protocol and a computer storage medium on which is stored instructions to enable general purpose computers to carry out the protocol.

Brief description of the drawings

For a better understanding of the invention and to show how the same may be carried into effect, there will now be described, by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

Fig 1 illustrates schematically transmission of encrypted data from a first to second computing entity;

Figure 2 illustrates schematically physical and logical resources of the computing entities illustrated in Fig 1;

Figure 3 illustrates schematically data communications between the computing entities of Figures 1 and 2;

Figures 4A to 4C illustrates schematically process steps carried out by the one of the computing entities of Figures 1 and 2; and

Figures 5A to 5C illustrates schematically process steps carried out by the other of the computing entities of Figures 1 and 2.

Detailed description of the best mode for carrying out the invention

There will now be described by way of example the best mode contemplated by the applicant for carrying out the invention. In the following description numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent however, to one skilled in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well-known methods and structures have not been described in detail so as not to unnecessarily obscure the present invention.

There will now be described with reference to Figs 1 to 4 herein a method and apparatus by which private components p,q of a public-key n may be verified according to a first specific implementation of the present invention.

Referring to Fig 1, there is illustrated schematically a pair of computing entities 102,104 configured for communicating electronic data with each other over a communications network, in this case the internet 106, by communicating data 108,110 to each other via the internet 106 in well known manner. Illustrated in Fig 1 is first computing entity 102, herein after referred to as entity A and a second computing entity 104 herein referred to as entity B. In the example illustrated in Fig 1, the first and second computing entities 102,104 are geographically remote from each other and whilst in the best mode herein, the communications network comprises the know internet 106, in other embodiments and implementations of the present invention the communications network could comprise any suitable means of transmitting digitized data between the computing entities. For example, a known Ethernet network, local area network, wide area network, virtual private circuit or public telecommunications network may form the basis of a communications medium between the computing entities 102,104.

The computing entities 102 and 104 have been programmed by storing on memory 205,207 programs read from computer program storage media 112,114, for example, a CD-ROM.

Referring now to Fig 2, there is illustrated schematically physical resources and logical resources of the computing entities A and B. Each computing entity comprises at least one data processing means 200,202, a memory area 203,205, a communications port 206,208, for communicating with other computing entities. There is an operating system 209,211, for example a known Unix operating system. One or more applications programs 212, 214 are configured for operating for receiving, transmitting and performing data processing on electronic data received from other computing entities, and transmitted to other computer entities in accordance with specific methods of the present invention. Optionally there is a user interface 215,217 which may comprise a visual display device, a pointing device, e.g. a mouse or track-ball device, a keypad, and a printer.

Under control of the respective application program 212,214, each of the computing entities 300, 301 is configured to operate according to a first specific method of the present invention.

Referring to Fig 3 herein, there is illustrated schematically data communications passed between the first and second computing entities to effect verification by B of A's

private components of a public-key according to the first specific implementation of the present invention.

Applications programs 212,214 operate a set of algorithms that effect implementation of the verification protocol. The precise implementation of the algorithms is preferably made n a conventional prior art programming language, for example the language C, or C++ using conventional programming techniques which are known to those skilled in the art. For a better understanding of the implementation of the algorithms, the following presents a model, notation and explanation of the verification protocol. It will be understood by those skilled in the art that the algorithmic steps are used to control the logical and physical resources of the computing entities by being programmed into the applications in a conventional programming language.

Referring now to Figures 3, 4 and 5, there will now be described the operation of two computing entities commonly referred to Alice and Bob which will be adopted here. The computing entity 102 and computing entity 104 by following the steps of Figures 4 and 5, respectively, exchanging signals representative of various data values as shown in Figure

First, the computing entities agree on a set of parameters as follows, where Alice 102 is the prover and Bob 104 is the verifier. Alice has constructed $n = pq$ such that p and q are distinct odd primes with $|\ell(p) - \ell(q)| \leq d$ (i.e., the lengths of the two primes differ by at most d bits). The length of n is generally at least 512 to meet common security standards. d is preferably no greater than 2 but can be larger. The disadvantage of a larger d is that as d increases it will reach a threshold where the probability of p and q are primes when the test of the present invention is passed becomes dependent on n not k.

A proof will be abandoned on Alice's instigation if any check she (i.e., the computing entity A) performs fails and will be rejected by Bob if any check he (ie the computing entity B) performs fails.

First, Alice shall help Bob to set up a multiplicative group of order n. For her part, Alice only needs to generate a prime P with $n|(P-1)$. This prime can be constructed by testing the primality of $P = 2\alpha n + 1$ for $\alpha = 1,2,\ldots$, until P is found to be prime. By the prime number theorem (general form due to Dirichlet, see e.g., p.28 of [E. Kranakis.

Primality and Cryptography, Wiley-Teubner Series in Computer Science, John Wiley & Sons, 1986]), for fixed n with $P = 2\alpha n+1 \le N$, there are roughly

$$\pi n(N) = \frac{2\alpha}{\ln(2\alpha n+1)}$$

Such P's which are under N and are primes. Note that $N \le 2\alpha n+1$ and $n > \phi(2n)$. So

$$\pi n(N) \approx \frac{1}{\phi(2n)} \cdot \frac{N}{\ln N}$$

Since Alice's primality test procedure uses $\alpha = 1,2,\ldots$, the above inequality indicates a non-trivial probability for two primes to show up upon α reaching $\ln(2n \ln n)$. So one can be sure that α is small (likely to be bounded by $\ln(2n \ln n)$). It will be computationally easy for Alice to find the prime P (step 402). Once P is found to be prime, Alice sends the numbers n and P to Bob (step 404, data 302).

Upon receipt of n and P (step 501), Bob tests the primality of P (step 502). If P is not a prime the proof is rejected (step 504). Upon passing of the test, Bob chooses a random element $f < P$ (step 506), and sets

$$g = f^{(P-1)/n} \bmod P \text{ (step 508)}$$

Bob then sends g to Alice (steps 510, data 304).

Upon receipt of g (step 406), Alice shall check $Ord_P(g) = n$ (step 408). If this does not hold, Alice may not be able to pass a proof later and so abandons the proof (step 410).

Above we have reasoned that $2\alpha = (P-1)/n$ is small ($<< n$). Thus, for $n = pq$, there can only be a few factors of $P-1$ which are less than n and are fully known to Alice. So it will be computationally easy for Alice to check $Ord_P(g) = n$. Upon passing this simple checking, Alice shall set

$$A = g^p \bmod P, \qquad B = g^q \bmod P \text{ (step 412).}$$

Alice then sends the pair (A, B) to Bob (step 414, data 306)

Upon receipt of (A, B)(step 512), Bob shall check the following:

$$A \neq B, A \neq 1, B \neq 1 \text{ (step 514).}$$

If these checks are passed, the system parameters have been properly set up and moves on to step 520. If not, Bob rejects the proof (step 518).

For clarity, we shall omit the trailing mod P operation in the following protocol specification which, for reference will be called Two_Prime_Product (n, g, A, B , P) The following steps are repeated k times

1. Bob picks $h \in Z_n^*$ at random with $\left(\frac{h}{n}\right) = -1$ (step 520) and sends it to Alice (steps 522, data 308).
2. Alice receives h (step 420) and checks $\left(\frac{h}{n}\right) = -1$ (step 422) and abandons the proof (step 424) if the check fails. If the check passes Alice, picks u, v at random (step 426) such that

$$\ell(u) = \ell((p-1)/2)$$
$$\ell(v) = \ell((q-1)/2)$$

and sets

$$U = g^{2u}, \quad V = g^{2v}, \quad H_U = B^{(h^u \bmod n)},$$

$$H_V = A^{(h^v \bmod n)}, H_{UV} = h^u h^v \bmod n \text{ (step 426);}$$

Alice sends to Bob: U, V, H_u, H_v, H_{uv} (steps 428, data 310).

3. Bob receives these values from A (step 524) and picks a challenge $c \in \{0,1\}$ at random (step 526) and sends it to Alice (steps 528, data 312).
4. Alice receives the challenge (step 430) and sends Bob the responses
   $r = u + c(p-1)/2, \quad s = v + c(q-1)/2$ (step 432, data 314).

5. Bob receives r and s from A (step 530) checks all of the following ($c = 0$);

5.1 $$\ell(r) \le \lfloor \ell(n)/2 \rfloor + 2, \quad \ell(s) \le \lfloor \ell(n)/2 \rfloor + 2$$

5.2 $$g^{2r+1} \equiv Ug, \quad g^{2s+1} \equiv Vg$$

5.3 $$B^{(h^r \bmod n)} \equiv H_U, \quad A^{(h^s \bmod n)} \equiv H_V$$

5.4 $$h^r h^s \equiv H_{UV} \pmod{n}$$

6. Bob checks: ($c = 1$)

6.1 $$\ell(r) \le \lfloor \ell(n)/2 \rfloor + 2, \quad \ell(s) \le \lfloor \ell(n)/2 \rfloor + 2$$

6.2 $$g^{2r+1} \equiv UA, \quad g^{2s+1} \equiv VB$$

6.3 $$B^{(h^r \bmod n)} \equiv H_U{}^{\pm 1}, \quad A^{(h^s \bmod n)} \equiv H_V{}^{\mp 1}$$

($H_U{}^{\pm 1}$ and $H_V{}^{\mp 1}$ means the exponents take opposite signs)

6.4 $$h^r h^s \equiv H_{UV} h^{(n-1)/2} \pmod{n}$$

at steps 534 or 536, for $c = 0$, $c = 1$, respectively.

If $c = 0$ and any of the checks of step 534 fails then Bob rejects the proof (step 536). Similarly, if $c = 1$ and if the checks of step 538 fail, then Bob rejects the proof (step 536).

If the checks at step 534 all pass, Bob decides if a primality check for a further value of n is required (step 540). If "Yes" Bob chooses another h(step 520) and another iteration is carried out; if "No" the protocol is ended (step 542).

If the checks at step 538 all pass, Bob checks for Monte-Carlo evidence at step 542 and then determines if another iteration is to be carried out (step 540).

Alice then determines if Bob wishes to go through a further iteration (step 434). If "Yes" it returns to step 420, if "No" the protocol ends.

We shall see below that the two congruences checked in step 6.3 actually evaluate the Jacobi (Legendre) symbols $\left(\frac{h}{p}\right)$ and $\left(\frac{h}{q}\right)$. Using challenges of the negative Jacobi symbol has the virture of not disclosing the quadratic residue information of the challenges. In contrast, many square-root displaying protocols (e.g., [R. Gennaro, D. Miccianicio and T. Rabin. An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products, In 5gh ACM Conference on Computer and Communications Security, October 1998, J. van de Graaf and R. Peralta. A simple and secure way to show the validity of your public-key, Advances in Cryptology – Proceedings of CRYPTO 87 (E. Pomerance, ed.), Lecture Notes in Computer Science, Springer-Verlag, 293 (1988),pp. 128-134]) disclose such information.

The protocol allows for the two factors to have size differences satisfying $|\ell(p) - \ell(q)| \leq d$. Larger size differences, if desirable, can be accommodated by adjusting the inequalities in steps 5.1 and 6.1.

We analyze the security the protocol, which consists of the properties of completeness, soundness, and privacy.

Completeness

Theorem 1 *If Alice follows the specification of Two_Prime_Product, a proof will be accepted.*

Proof We show that Bob will be satisfied by the checks performed in protocol step 5.1 through step 5.4.

First, we show the inequalities in 5.1. Alice has set p and q such that $pq = n$

$$-2 \leq \ell(p) - \ell(q) \leq 2. \tag{1}$$

Obviously

$$\ell(n) \leq \ell(p) + \ell(q) \leq \ell(n) + 1. \tag{2}$$

Adding (1) to (2) yields

$$2\ell(p) \leq \ell(n) + 3,$$

or

$$\ell(p) \leq \lfloor \ell(n) \rfloor / 2 + 2. \tag{3}$$

Alice has chosen $\ell(u) = \ell((p-1)/2)$. With p odd, $(p-1)/2$ is a whole number and $\ell((p-1)/2) = \ell(p) - 1$. So when $c = 0$

$$\ell(r) = \ell(u) = \ell((p-1)/2) = \ell(p) - 1,$$

and When $c = 1$

$$\ell(r) = \ell(u + (p-1)/2) \leq \ell((p-1)/2) + 1 = \ell(p).$$

So for both cases, (3) will imply

$$\ell(r) \leq \lfloor \ell(n) \rfloor / 2 + 2.$$

Analogously we can show

$$\ell(s) \leq \lfloor \ell(n) \rfloor / 2 + 2.$$

In the following, we shall only examine the cases under $c = 1$, since $c = 0$ will render the congruences in 5.2 through 5.4 to hold trivially.

In 5.2, noting that $g^p \equiv A \pmod P$ and the structures of U and r, it is easy to see that the first congruence will hold. The second congruence holds similarly.

To see that the congruences in 5.3 will hold, observe

$$B^{(h^{(p-1)/2} \bmod n)} \equiv B^{(h^{(p-1)/2} \bmod p)} \equiv B^{\left(\frac{h}{p}\right)} \pmod P. \tag{4}$$

The first congruence in (4) is due to $Ord_P(B) = p \mid n$. Then, since p is prime, the second congruence in (4) follows from Euler's criterion. Therefore, the first congruence in 5.3 (for $c = 1$) is:

$$\begin{aligned} B^{(h^r \bmod n)} &\equiv B^{(h^u + (p-1)/2 \bmod n)} \\ &\equiv (B^{(h^{(p-1)/2} \bmod n)})^{(h^u \bmod n)} \\ &\equiv (B^{(h^{(p-1)/2} \bmod p)})^{(h^u \bmod n)} \\ &\equiv (B^{\left(\frac{h}{p}\right)})^{(h^u \bmod n)} \\ &\equiv (B^{(h^u \bmod n)})^{\left(\frac{h}{p}\right)} \\ &\equiv H_U^{\left(\frac{h}{p}\right)} \pmod P, \end{aligned}$$

while the second congruence in 5.3 (for $c = 1$) is, analogously,

$$A^{(h^s \bmod n)} \equiv H_V^{\left(\frac{h}{q}\right)} \pmod P.$$

The exponents of the both right-hand sides must take opposite signs since Jacobi symbols only take values ± 1 and h has been chosen to satisfy

$$-1 = \left(\frac{h}{n}\right) = \left(\frac{h}{p}\right)\left(\frac{h}{q}\right).$$

Therefore the congruences in 5.3 will hold.

Finally, any $h \in Z_n^*$ will satisfy

$$h^{p+q} \equiv h^{n+1} \pmod n.$$

With $(p-1)/2$, $(q-1)/2$ and $(n-1)/2$ being whole numbers, it is easy to rewrite the above into

$$h^{[(p-1)/2 + (q-1)/2]} \equiv h^{(n-1)/2} \pmod n.$$

Therefore the congruence in 5.4 will hold. □

Soundness

We now show that protocol Two_Prime_Product provides a Monte-Carlo method for testing the primality of the orders of A and B. We firstly note that all the numbers and variables to appear in this section are non-negative integers. In particular, $\log_g(A)$ and $\log_g(B)$ denote some positive integers p and q less than $Ord_P(g)$ satisfying $A \equiv g^p \pmod P$ and $B \equiv g^q \pmod P$.

Lemma 1 *Without the knowledge of the factorization of n, the element g fixed by Bob satisfies*

$$Pr[\ Ord_P(g)\ \textit{divides}\ x\ ] = x/n,$$

for any x divides n.

Proof Without the knowledge of the factorization of n, Bob's procedure for fixing g is via $g = f^{(P-1)/n} \bmod P$ using f which is chosen at random from Z_P^* (review Section 2.2). Then $g^n \equiv 1 \,(\mathrm{mod}\, P)$ by Fermat's Theorem. In the cyclic group Z_P^* there are exactly $n = \sum_{d|n} \phi(d)$ elements of orders dividing n. Only these elements can be the candidates for g. For the same reason, for any $x \mid n \mid P-1$, there are exactly $x = \sum_{d|x} \phi(d)$ elements in Z_P^* of orders dividing x. The claimed probability is thus calculated as that of picking x objects from n. □

Lemma 2 *Denote $Ord_P(B) = x$ and $Ord_P(A) = y$. Upon acceptance of a proof on running* Two_Prime_Product(n, g, A, B, P), *Bob accepts that his random choice of h in the protocol run ($(h,n) = 1$ and $\left(\frac{h}{n}\right) = -1$) satisfies*

$$\begin{cases} h^{[(\log_g(A)-1)/2]} \equiv \pm 1 \,(\mathrm{mod}\, x) \\ h^{[(\log_g(B)-1)/2]} \equiv \mp 1 \,(\mathrm{mod}\, y) \end{cases},$$

and the probability for failing this does not exceed $1/2^k$ where k is the number of iterations used in the protocol.

Proof The first congruence in 5.2 shows that Alice knows both $\log_g(U)$ (shown when $c = 0$) and $\log_g(UA) = \log_g(U) + \log_g(A)$ (shown when $c = 1$), and has added $\log_g(A)$ to the response whenever $c = 1$ is the case. Suppose Alice does not know $\log_g(A)$. Then in each iteration she can only answer Bob's random challenge with at most $1/2$ chance of correctness. Thus, after having verified k times of correct responses to his random challenges, Bob should agree that the probability for Alice not having used $\log_g(A)$ in her response (when $c = 1$) is at most $1/2^k$.

The first congruence in 5.3 further shows that H_U is generated from B with the use of an exponent which is in turn generated from Bob's randomly chosen challenge h. Since $(h, n) = 1$, $(h^r \bmod n,\ n) = 1$. Therefore

$$Ord_P(H_U) = Ord_P(B) = x.$$

Clearly, the quantity $\log_g(A)$ in $2r + 1$ (when $c = 1$) amounts to $(\log_g(A) - 1)/2$ in r. Therefore the first congruence in 5.3 shows that for h satisfying $(h, n) = 1$:

$$h^{[(\log_g(A)-1)/2]} \equiv \pm 1 \,(\mathrm{mod}\, x).$$

Analogously we can use the second congruence in 5.3 to establish that for the same h

$$h^{[(\log_g(B)-1)/2]} \equiv \mp 1 \,(\mathrm{mod}\, y).$$ □

In the rest of this section we will continue denoting

$$Ord_P(B) = x, \quad Ord_P(A) = y.$$

Following the Solovay-Strassen primality test technique [17] we define the following set

$$H_x = \{\, h \in Z_x^* \mid (h,x) = 1,\ \ h^\alpha \equiv \pm 1 \,(\mathrm{mod}\, x),\ \ \alpha \text{ constant} \,\}. \tag{5}$$

Clearly, this set is a subgroup of Z_x^*. It is a variation of its counterpart used in the Solovay-Strassen primality test technique. There, H_x is defined such that the exponent α is $(x-1)/2$. In our "test in the dark" method, the verifier Bob is not given the modulus x, let alone does he know the relation between the exponent and the modulus. All the information Bob has is that the modulus is a factor of n, and that the exponent is a constant. (The result of Lemma 2 stipulates the constant be $(\log_g(A)-1)/2$.)

Lemma 3 *Let x, y and h be as in Lemma 2. Bob accepts that x and y are prime powers. The probability for failing this does not exceed $1/2^k$.*

Proof We prove the lemma by estimating the probability for x not being a prime power. A prime power can be written as p^r with p prime and $r \geq 1$. Suppose x is not a prime power. Then let $x = \xi\eta$ with $\xi > 1$, $\eta > 1$ and $(\xi,\eta) = 1$.

Obviously, either H_x is a proper subgroup of Z_x^*, or $H_x = Z_x^*$.

In the first case, $\#H_x$ is at most half of $\#Z_x^*$ (since the former must divide the latter), and thereby the probability for each h randomly picked from Z_x^* to fall in H_x cannot exceed $1/2$, which amounts to $1/2^k$ to bound the probability for k such h's to be so.

Now we consider $H_x = Z_x^*$. We claim that H_x will only contain elements satisfying

$$h^\alpha \equiv 1 \,(\mathrm{mod}\, x), \tag{6}$$

where α is the constant in (5). Suppose $H_x = Z_x^*$ while (6) is not true for some element in H_x. Let h be such an element. So $h^\alpha \equiv -1 \,(\mathrm{mod}\, x)$. Since ξ and η are relatively prime, by the Chinese remainder theorem, the system $f \equiv 1 \,(\mathrm{mod}\, \xi)$, $f \equiv h \,(\mathrm{mod}\, \eta)$ has a solution $f \in Z_x^*$. Obviously,

$$f^\alpha \equiv 1 \,(\mathrm{mod}\, \xi), \qquad f^\alpha \equiv -1 \,(\mathrm{mod}\, \eta),$$

yielding

$$f^\alpha \not\equiv \pm 1 \,(\mathrm{mod}\, x).$$

So $f \in Z_x^* \setminus H_x$, contradiction to $H_x = Z_x^*$.

So now we must consider $H_x = Z_x^*$ with all elements in H_x satisfying (6). This implies that for k randomly chosen h's with $(h \bmod y,\, y) = 1$, $h^\beta \equiv -1 \,(\mathrm{mod} y)$ where $\beta = (\log_g(B) - 1)/2$. Let z be a prime factor of y. Then we will also have $(h^\beta \bmod z,\, z) = 1$ and

$$h^\beta \equiv -1 \,(\mathrm{mod}\, z). \tag{7}$$

Since z is prime, by Fermat's Theorem we know $z - 1 \mid 2\beta$, i.e., β is a multiple of $(z-1)/2$. In Z_z^* there are exactly half the elements which are quadratic non-residues satisfying (7) (none of other elements can satisfy it). So the probability for this

congruence to hold for k randomly chosen h's cannot exceed $1/2^k$. This value must also bound the probability for x not being a prime power.

By symmetry, y is also a prime power. □

Lemma 4 *Under the hypotheses of Lemma 3, $(x, y) = 1$, and the probability for failing this does not exceed $1/2^k$.*

Proof Since x and y are both prime powers, if $(x, y) > 1$, we can assume without loss of generality that $x = p^r \mid y$. Using the result of Lemma 2 we can derive

$$\mp 1 \equiv h^{\beta} (\bmod\, y) \equiv h^{\beta} (\bmod\, x).$$

At the same time we have

$$h^{\alpha} \equiv \pm 1 \,(\bmod\, x).$$

Thus,

$$h^{|\alpha-\beta|} \equiv -1 \,(\bmod\, x) \equiv -1 \,(\bmod\, p),$$

for all k instances of randomly-picked h with $(h, p) = 1$. Since p is prime, the above is only possible if $p - 1$ divides $2|\alpha - \beta|$ but not divides $|\alpha - \beta|$. So $|\alpha - \beta|$ is an odd multiple of $(p - 1)/2$ which implies

$$h^{(p-1)/2} \equiv -1 \,(\bmod\, p) \tag{8}$$

for all such h mod p. There are only half the elements in Z_p^* which are quadratic non-residues satisfying (8). Therefore the probability for (8) to hold for k time, i.e., for k random h's with h mod p being quadratic non-residues will not exceed $1/2^k$. Since the congruence in (8) is derived from the assumption $(x, y) > 1$, the value $1/2^k$ also bounds the probability for $(x, y) > 1$. □

Lemma 5 *Under the hypotheses of Lemma 2, there exists integers a and b satisfying*

$$\log_g(A) = ax \leq 8n^{1/2}, \quad \log_g(B) = by \leq 8n^{1/2}.$$

Proof From the proof of Lemma 2 we know that A is generated from g. So its order y can only be reduced from $Ord_P(g)$ and thereby $y \mid Ord_P(g)$. We also know

$$0 \equiv \log_g(1) \equiv \log_g(A^y) \equiv y \log_g(A) (\bmod\, Ord_P(g)).$$

This means

$$Ord_P(g) \mid y \log_g(A). \tag{9}$$

By symmetry, $x \mid Ord_P(g) \mid x \log_g(B)$. Then $xy \mid Ord_P(g)$ since $(x, y) = 1$ (Lemma 4). Combining this with (9), we have $x \mid \log_g(A)$. By symmetry we can also derive

$$Ord_P(g) \mid x \log_g(B), \tag{10}$$

and $y \mid \log_g(B)$. So we can write

$$\log_g(A) = ax, \quad \log_g(B) = by,$$

for some a and b.

In protocol step 5.1. Bob has checked that in both challenge cases, the responses r and s satisfy

$$\ell(r) \leq \lfloor \ell(n)/2 \rfloor + 2.$$

Since when the challenge is $c = 1$, $\ell(\log_g(A)) \leq \ell(2r+1) = \ell(r) + 1$,

$$\ell(\log_g(A)) \leq \lfloor \ell(n)/2 \rfloor + 3.$$

This implies

$$\log_g(A) \leq 2^{\lfloor \ell(n)/2 \rfloor + 3} \leq 8n^{1/2}.$$

By symmetry, $by = \log_g(B) \leq 8n^{1/2}$. □

Now we can prove the soundness of our protocol.

Theorem 2 *Upon acceptance of a proof* Two_Prime_Product(n, g, A, B, P) *with* $n \geq 24^4$ *and odd, Bob accepts that* $\log_g(A)$ *and* $\log_g(B)$ *are distinct odd primes. The probability for failing this does not exceed* $\max(1/2^k, 24/n^{1/4})$ *where* k *is the number of iterations used in the proof.*

Proof We know $x \neq y$ since they are relatively prime to each other. Both are odd since both divide an odd number n. By symmetry, we only need to prove the case for $x = \log_g(A)$ to be a prime. We have already established $ax = \log_g(A)$ (Lemma 5) and $x = p^r$ with p being prime (Lemma 3). So to prove this theorem we need only to show $a = r = 1$. We shall establish the probability for Bob to accept the proof while assuming either $r > 1$, or $a > 1$. Using the method that we have used in the proof of Lemma 3, we shall reason that if any of these two cases is true, then either H_x (defined in (5)) should be a proper subgroup of Z_x^*, which will render $1/2^k$ to bound the probability for Bob to accept a proof of k iterations, or another event of a negligibly small probability should has occurred.

First, consider the case of $r > 1$.

There exists $h \in Z_{p^r}^*$ of the full order $(p-1)p^{r-1}$. This element cannot be in H_x since otherwise the first congruence established in Lemma 2 will imply

$$h^{ap^r - 1} \equiv 1 \pmod{p^r},$$

which yields

$$(p-1)p^{r-1} \mid ap^r - 1.$$

So there exists λ satisfying

$$ap^r - \lambda(p-1)p^{r-1} = 1.$$

This means p^{r-1} is relatively prime to p^r, impossible with $r > 1$. So H_x must be a proper subgroup of Z_x^*.

The remaining case is $a > 1$ and x prime.

There exists $h \in Z_x^*$ of full order $x-1$. If h is not in H_x then H_x is a proper subgroup and we have done. Now suppose $h \in H_x$. The first congruence in Lemma 2 implies

$$h^{ax-1} \equiv 1 \,(\mathrm{mod}\, x),$$

which further implies $x-1 \,|\, ax-1 = a(x-1)+a-1$. So $x-1 \,|\, a-1$. This is only possible if $x \leq a$. From Lemma 5, $ax \leq 8n^{1/2}$. So $x^2 \leq ax \leq 8n^{1/2}$, or $x < 3n^{1/4}$. Lemma 5 also requires $\log_g(B) = by \leq 8n^{1/2}$. These yield

$$x \log_g(B) = xby < 24n^{3/4}.$$

So, this case of $\log_g(A)$ requires $xby < 24n^{3/4}$. From (10), $Ord_P(g) \,|\, xby$. Also, $Ord_P(g) \,|\, n$. So $Ord_P(g) \,|\, (xby, n) \leq xby \leq n$ $(n \geq 24^4)$. Now we can apply Lemma 1 and obtain

$$Pr[\ Ord_P(g) \text{ divides } (xby, n)\ ] = (xby, n)/n \leq xby/n < 24/n^{1/4}.$$

We have shown that if x is not a prime, or $x \neq \log_g(A)$, then the probabilities for Bob to accept the proof are bounded by either $1/2^k$, or $24/n^{1/4}$, whichever is larger. The latter value bounds the probability for Bob to have chosen g of such a small order. □

Remark In the proof of Theorem 2 and Lemma 3 we have used random elements in Z_x^*. We should point out that in the protocol Bob only picks h at random from Z_n^*, rather than from Z_x^*, since he does not know the factorization of n. Also h is chosen to have the negative Jacobi symbol mod n. However, the mapping from such h in Z_n^* to h mod x in Z_x^* is *onto* (the mapping is accomplished by the double exponentiations checked in protocol step 5.3) and thereby results in uniformly distributed elements in Z_x^*.

Theorem 3 *Under the hypotheses of Theorem 2,* $n = \log_g(A)\log_g(B)$, *and the probability for failing this does not exceed* $\max(1/2^k, 8/n^{1/4})$.

Proof In Theorem 2 we have proved $\log_g(A)\log_g(B) = xy = Ord_P(g) \,|\, n$ where x and y are distinct primes. Suppose $n = xyz$ for some integer z. We prove the theorem by estimating the probability for $z > 1$.

The congruence checked in protocol step 5.4 implies that each h that Bob chooses at random satisfies

$$Ord_n(h) \,|\, n - x - y + 1 \tag{11}$$

Define the following set as a subgroup of Z_n^*:

$$H = \{\ h \in Z_n^* \mid h^{(n-x-y+1)} \equiv 1 \,(\mathrm{mod}\, n)\ \}.$$

Since x, y are distinct primes, there exists $h \in Z_n^*$ of order $\max(x-1, y-1)$. If $h \notin H$ then H is a proper subgroup of Z_n^* and $\#H$ cannot exceed the half of $\#Z_n^*$. Thus, the probability for choosing k random elements from Z_n^* which also fall in H (to pass the congruence in step 5.4) will not exceed $1/2^k$.

Now suppose $h \in H$. Without loss of generality, let $x-1 \geq y-1$. Then from (11) we can derive

$$x - 1 = Ord_n(h) \mid z - 1.$$

This is only possible if $x \leq z$. Given $y \leq 8n^{1/2}$, the maximum possible value for $Ord_P(g) = xy = n/z$ can only be resulted from the maximum possible value of $x = z$, which renders

$$Ord_P(g) = xy \leq 8n^{3/4}.$$

Applying Lemma 1 we know that the probability for Bob having chosen g of such a small order does not exceed $8/n^{1/4}$.

Thus, we can use $\max(1/2^k, 8/n^{1/4})$ to bound the probability for $z > 1$. □

To this end we know that the two primes factors of n have roughly equal size since

$$\log_g(A) \leq 8n^{1/2}, \quad \log_g(B) \leq 8n^{1/2}.$$

As a concluding remark for our soundness analysis, we emphasize the importance of verifying the congruences in the protocol step 5.3. Besides their roles in the soundness proof that we have seen, they also exclude x and y from being certain pseudo-primes such as Carmichael numbers (see e.g., p.137 of [13]). Moreover, they prevent x and y from being methodically chosen in a cheating way that can pass a (flawed) protocol in [12] for proof of a required format for RSA moduli. (The required format is the same as what our protocol proves: n is the product of exactly two primes of roughly equal size.) That protocol first applies a square-root displaying protocol to prove that n is the product of two prime powers ([12] suggests to use the method of [9] for proof of Blum integers; we will discuss more on square-root displaying protocols in Section 4), and then verifies

$$h^{x+y} \equiv h^{n+1} (\mathrm{mod}\, n)$$

(equivalent to the congruence checked in our protocol step 5.4), plus checking the sizes of x and y. Below we reason that such verification does not suffice for proving the required format of n.

Let $n = xy$ with x, y being odd. It is easy to see that, as long as $\lambda(n)$ (Carmichael function of n, which is the lowest order of all elements in Z_n^*) divides $(x-1)(y-1)/2 = (n-1)/2 - [(x-1)+(y-1)]/2$, the congruence above will always pass. Alice can thus cheat as follows. She sets $x = p^r$ with p prime and $r > 1$ such that $y = 2p^{r-1} + 1$ is prime and $\ell(x) \approx \ell(y)$. There are sufficiently many primes p such that $2p^{r-1} + 1$ is also prime. So it will be easy for Alice to find p and y to satisfy what is required. Clearly, n is the product of two prime powers, and will therefore pass a Blum integer proof based on displaying square roots of challenges. The size checking on x and y will pass too. Moreover,

$$(x-1)(y-1) = (p^r - 1)2p^{r-1} = (p-1)(...)2p^{r-1},$$

and

$$\lambda(n) = \mathrm{lcm}(\phi(x), \phi(y)) = \mathrm{lcm}((p-1)p^{r-1}, 2p^{r-1}) = (p-1)p^{r-1}.$$

So it always holds

$$\lambda(n) \mid (x-1)(y-1)/2.$$

Consequently, verification using $h^{x+y} \equiv h^{n+1} (\mathrm{mod}\, n)$ will pass for all $h \in Z_n^*$. But n is not the product of exactly two primes, and the sizes of its prime factors are not roughly equal ($\ell(p) \approx \ell(y)/r$).

Privacy

In addition to n Alice has also made available the following two constants:

$$(A, B) \equiv (g^p, g^q) \,(\mathrm{mod}\, P).$$

Were these two constants not available, the prime factors of n are protected by the factorization problem. On the other hand, were n not available, given the two constants (A, B) to find (p, q) one faces the discrete logarithm problem. Our privacy analysis shall nevertheless identify whether finding p and q will still remain a hard problem given the availability of both n and (A, B). Clearly, we can no longer consider the problem to be those of pure factorization or pure discrete logarithm.

To identify the exact difficulty for finding p, q from n and (A, B), suppose there exists an efficient algorithm $\mathcal{A}$ such that with input (g, A, B, n) it will output p and q in time bounded by a polynomial in the size of n. We should keep in mind that $\mathcal{A}$ works because the input values are related by

$$n \equiv \log_g(A) \log_g(B) \,(\mathrm{mod}\, n). \tag{12}$$

Were the input values not related in any way then because to date there exists no polynomial-time algorithms to factor integers or to compute discrete logarithms, $\mathcal{A}$ should not have output $\log_g(A)$, $\log_g(B)$ in time bounded by any polynomial in the size of n.

For any z with $(z, n) = 1$, (12) is equivalent to

$$n \equiv [z \log_g(A)][z^{-1} \log_g(B)] \equiv \log_g(A^z) \log_g(B^{z^{-1}}) \,(\mathrm{mod}\, n).$$

So with input $(g, A^z, B^{z^{-1}}, n)$ $\mathcal{A}$ should output $\log_g(A^z)$ and $\log_g(B^{z^{-1}})$ in time bounded by a polynomial in the size of n.

Further notice that for any $z < q$, $A' \equiv A^z (\mathrm{mod}\, P)$ forms a permutation in the subgroup generated by A. Analogously for any $z' < p$, $B' \equiv B^{z'} (\mathrm{mod}\, P)$ forms a permutation in the subgroup generated by B. Thus, given an arbitrary quadruple $(g, A', B', 1)$, $\mathcal{A}$ forms a decision procedure to answer whether $(g, A', B', 1)$ is a member of the Diffie-Hellman quadruples generated by g.

Theorem 4 *Under the assumptions that factorization of n and computing discrete logarithms to the base g are infeasible, finding p, q, from the constants A, B and the modulus n is at least as difficult as solving a decision problem on the membership of the Diffie-Hellman quadruples generated by g.* □

This membership decision problem is often referred to as Decision-Diffie-Hellman Problem ([15, 18]) and is widely regarded hard.

Performance

The operations in the protocol mainly involve exponentiations modulo big integers and evaluation of Jacobi symbols. Because the cost of the latter is trivial in comparison to that of the former, we shall focus our attention of estimating the cost of modulo exponentiations.

We shall not consider the cost for Alice to generate n and the related prime $P = 2\alpha n + 1$ since these procedures are purely local to Alice (while a protocol involves communications). She can prepare these two numbers well in advance before running the protocol. However, the cost to Bob of testing the primality of P should be included in the cost for him to run the protocol.

Testing the primality of P using a Monte-Carlo method needs k testing iterations to achieve $1/2^k$ error probability (using k the same as that in the protocol to equalize the error probability). Each iteration mainly involves exponentiation mod P so for this part, Bob performs k exponentiations mod P.

In the proof protocol, in each iteration Alice computes four exponentiations mod P and two of them mod n. Bob performs slightly more: four of them mod P and on average 2.5 of them mod n (2 for $c = 0$ and 3 for $c = 1$). Thus, with a proof of k iterations, Alice computes $4k$ exponentiations mod P and $2k$ of them mod n. For Bob's part adding the cost of testing the primality of P, he should perform in total $5k$ exponentiations mod P and 2.5 of them mod n.

Notice the fact that $P = 2\alpha n + 1$ where α is small (at the level of $\ln(2n \ln n)$, see Section 3.2). We have

$$\log_2 P - \log_2 n \approx \log_2[2\ln(2n \ln n)]$$

This means that the size of P may exceed that of n by only a few bits (for instance for any n of size less than 10,000 bits, $\log_2[2\ln(2n \ln n)] < 5$, which is less than two percent of the size of n). Since the previous equation renders that the growth of the size difference between the two moduli is much slower than that of the moduli, we can claim that for n any size larger than 512 bits (recommended least size for today), the size of P will not exceed that of n by two percent (of the size of n), namely

$$\log_2 P \le 1.02 \log_2 n .$$

Since in bit operation, the cost for exponentiation mod P is measured in $O((\log_2 P)^3)$, i.e., $C(\log_2 P)^3$ for some constant C, we can use the following to relate the cost of exponentiation mod P to that mod n (of any size larger than 512 bits):

$$(\log_2 P)^3 \le (1.02 \log_2 n)^3 \approx 1.062(\log_2 n)^3$$

That is, the cost of one exponentiation mod P will not exceed that of one mod n by seven percent. We nevertheless use a ten percent expansion and convert Bob's workload of $5k$ exponentiations mod P into $5.5k$ exponentiations mod n. So in total Bob will need to compute no more than $7k$ of them. Since on average an exponentiation mod n amunts to $1.5\log_2 n$ multiplications mod n, the total cost to Bob for running the protocol will be $12k\log_2 n$ multiplications of integer of size n. We can also use this quantity to bound Alice's cost of running the protocol.

For n of size larger than 512 bits, the computational cost of proving and verifying that n is the product of two primes of roughly equal size using protocol Two_Prime_Product is $12k\log_2 n$ multiplications of integer of size of n. Both parties should perform this number of operations.

Considering the fact that a Monte-Carlo primality test on non-secret number mainly involves modulo exponentiation, Bob's verification cost is equal to eight such tests on non-secret numbers of size n.

We have constructed an efficient knowledge proof protocol for demonstrating an integer being the product of two prime factors of roughly equal size. The new protocol is the first of its kind that proves such a structure with efficiency comparable to that of a Monte-Carlo method for primality evidence "in the dark".

Previous techniques for proving such a structure have a much higher cost for non-Blum integers (as will be discussed below). The improved efficiency for reasoning about non-Blum integers due to this work manifests a particular suitability for using the proposed protocol in the proof of valid RSA keys which are generated at uniformly random (e.g., for the protocol of Blackburn and Galbraith (S.R. Blackburn and S.D. Galbraith. Certification of secure RSA keys, University of Waterloo Centre for Applied Cryptographic Research, Technical Report CORR 90-44, Avalailable from `http://www.cacr.math.uwaterloo.ca/1]`).

The cost of a proof amounts to $12k\log_2 n$ multiplications of integers of size of n where k is the number of the iterations in the proof and relates to an error probability bounded by $\max(1/2^k, 24/n^{1/4})$. This is the first protocol that proves the two-prime-product structure of a number with the cost at the level of $O(k\log_2 n)$ multiplications and the error probability at the level of $1/2^k$ (considering $k = 60$, and $n > 2^{512}$, $1/2^k >> 24/n^{1/4}$) regardless of whether the number in question is a Blum integer [M. Blum. Coin flipping by telephone: a protocol for solving impossible problems, Proceedings of *24th IEEE Computer Conference (CompCon)*, 1982, pp. 133-137].

CLAIMS

1. A method of exchanging digital public-key verification data whereby a first party enables a second party to obtain probabilistic evidence that a given public-key number n is the product of exactly two odd primes p and q, not know to the second party, whose bit lengths ($\ell(p), \ell(q)$) differ by not more than d bits; the method including the following steps, all operations being to mod P unless specified mod n, the method being halted should any check fail;

a) said first party provides to said second party a number P such that P is a prime number and $n|(P-1)$;

b) said second party provides to said first party a number g where $g = f^{(P-1)/n} \bmod P$, $f < P$;

c) said first party provides to said second party numbers A and B, where $A = g^p \bmod P$ and $B = g^q \bmod P$;

d) said second party checks that $A \neq B, A \neq 1$ and $B \neq 1$; whereupon the following steps are repeated up to k times;

e) said second party selects a random number $h \in Z_n^*$ such that $\left(\frac{h}{n}\right) = -1$ and provides the number h to the first party;

f) said first party checks that $\left(\frac{h}{n}\right) = -1$ and selects two random numbers u and v such that $\ell(u) = \ell((p-1)/2)$, $\ell(v) = \ell((q-1)/2)$ and provides to said second party the values $U = g^{2u}$, $V = g^{2v}$, $H_U = B^{\left(h^u \bmod n\right)}$, $H_V = A^{\left(h^v \bmod n\right)}$, and $H_{UV} = h^u h^v \bmod n$;

g) said second party sends a request to the first party that the first party provides to the second party values r and s, which the second party randomly specifies should be either:

(1) $r = u$ and $s = v$; or

(2) $r = u + (p-1)/2$, $s = v + (q-1)/2$

h) said first party provides the requested values r and s to the second party,

i) if the second party requested $r = u$ and $s = v$, the second party determines whether:

(1) $\ell(r) \le \lfloor \ell(n)/2 \rfloor + d, \quad \ell(s) \le \lfloor \ell(n)/2 \rfloor + d$,

(2) $g^{2r+1} \equiv Ug, \quad g^{2s+1} \equiv Vg$,

(3) $B^{(h^r \bmod n)} \equiv H_U, \quad A^{(h^s \bmod n)} \equiv H_V$, and

(4) $h^r h^s \equiv H_{UV} \pmod{n}$;

thereby verifying the values provided by the first party to the second party are as were required by steps a) to f); or, if the second party requested $r = u + (p-1)/2$, $s = v + (q-1)/2$, the second party determines whether:

(1) $\ell(r) \le \lfloor \ell(n)/2 \rfloor + d, \quad \ell(s) \le \lfloor \ell(n)/2 \rfloor + d$,

(2) $g^{2r+1} \equiv UA, \quad g^{2s+1} \equiv VB$,

(3) $B^{(h^r \bmod n)} \equiv H_U^{\pm 1}, \quad A^{(h^s \bmod n)} \equiv H_V^{\mp 1}$ ($\pm$ *and* $\mp$ meaning the two exponents are of opposite sign), and

(4) $h^r h^s \equiv H_{UV} h^{(n-1)/2} \pmod{n}$,

thereby obtaining said probabilistic evidence on whether the given public-key number n is the product of exactly two odd primes p and q whose bit lengths ($\ell(p)$, $\ell(q)$) differ by not more than d bits.

2. A method as claimed in claim 1 in which $d \le 2$.

3. A method as claimed in claim 1 in which at least one of the selections of random numbers or choice of r and s is uniformly distributed.

4. A computing entity comprising:

a data processing equipment

a memory; and

a communications equipment,

said data processing equipment being configured so as to be capable of processing data according to a set of instructions stored in said memory;

said communications equipment configured so as to communicate data according to

said set of instructions such that the computing entity is configured to

a) receive from another computing entity a number P such that P is a prime number and $n|(P-1)$;

b) provide to said other computing entity a number g where $g = f^{(P-1)/n} \bmod P$, $f< P$;

c) receive from said other computing entity numbers A and B, where $A = g^p \bmod P$ and $B = g^q \bmod P$;

d) check that $A \neq B, A \neq 1$ and $B \neq 1$, and, if correct, repeat up to k times;

e) select a random number $h \in Z_n^*$ such that $\left(\frac{h}{n}\right) = -1$ and provide the number h to said other computing entity;

f) receive from said other computing $U = g^{2u}$, $V = g^{2v}$, $H_U = B^{(h^u \bmod n)}$, $H_V = A^{(h^v \bmod n)}$, and $H_{UV} = h^u h^v \bmod n$ entity were u and v are two random numbers such that $\ell(u) = \ell((p-1)/2)$, $\ell(v) = \ell((q-1)/2$;

g) request the other computing entity to provide values r and s, randomly specified to be either:

(1) $r = u$ and $s = v$; or

(2) $r = u + (p-1)/2$, $s = v + (q-1)/2$;

h) receive the requested values r and s from the other computing entity,

i) if $r = u$ and $s = v$ was requested, determine whether:

(1) $\ell(r) \leq \lfloor \ell(n)/2 \rfloor + d$, $\ell(s) \leq \lfloor \ell(n)/2 \rfloor + d$,

(2) $g^{2r+1} \equiv Ug$, $g^{2s+1} \equiv Vg$,

(3) $B^{\left(h^r \bmod n\right)} \equiv H_U$, $A^{\left(h^s \bmod n\right)} \equiv H_V$,

and

(4) $h^r h^s \equiv H_{UV} \pmod n$;

thereby verifying the values provided by the other computing entity are as were required by steps a) to i); or , if $r = u + (p-1)/2$, $s = v + (q-1)/2$ was requested, determine whether:

(1) $\ell(r) \leq \lfloor \ell(n)/2 \rfloor + d$, $\ell(s) \leq \lfloor \ell(n)/2 \rfloor + d$,

(2) $g^{2r+1} \equiv UA, \quad g^{2s+1} \equiv VB$,

(3) $B^{(h^r \bmod n)} \equiv H_U{}^{\pm 1}, \quad A^{(h^s \bmod n)} \equiv H_V{}^{\mp 1}$ ($\pm$ *and* $\mp$ meaning the two exponents are of opposite sign), and

(4) $h^r h^s \equiv H_{UV} h^{(n-1)/2} \pmod{n}$

thereby obtaining said probablistic evidence on whether the given public-key number n is the product of exactly two odd primes p and q whose bit lengths ($\ell(p)$, $\ell(q)$) differ by not more than d bits.

5. A method as claimed in claim 4 in which $d \leq 2$.

6. A method as claimed in claim 4 in which at least one of the selections of random numbers or choice of r and s is uniformly distributed.

7. A computing entity comprising:

a data processing equipment

a memory; and

a communications equipment,

said data processing equipment being configured so as to be capable of processing data according to a set of instructions stored in said memory;

said communications equipment configured so as to communicate data according to said set of

instructions such that the computing entity is configured to:

a) provide to another computing entity a number P such that P is a prime number and $n|(P-1)$;

b) receive from the other computing entity a number g where $g = f^{(P-1)/n} \bmod P$, $f < P$;

c) provide to said other computing entity numbers A and B, where $A = g^p \bmod P$ and $B = g^q \bmod P$;

d) receive from said other computing entity a random number $h \in Z_n^*$ such that $\left(\frac{h}{n}\right) = -1$;

e) check that $\left(\frac{h}{n}\right) = -1$ and, if so, select two random numbers u and v such that $\ell(u) = \ell((p-1)/2)$, $\ell(v) = \ell((q-1)/2)$ and provide to said other computing entity the values $U = g^{2u}$, $V = g^{2v}$, $H_U = B^{(h^u \bmod n)}$, $H_V = A^{(h^v \bmod n)}$ and $H_{UV} = h^u h^v \bmod n$;

f) receive from said other computing entity a request to provide to said other computing entity values r and s, which said other computing entity randomly specifies should be either:

(1) $r = u$ and $s = v$; or

(2) $r = u + (p-1)/2$, $s = v + (q-1)/2$

g) provide the requested values r and s to said other computing entity.

8. A method as claimed in claim 7 in which $d \leq 2$.

9. A method as claimed in claim 7 in which at least one of the selections of random numbers uniformly distributed.

10. A system of co-operating computer entities including a first computing entity as claimed in claim 4 and a second computing entity as claimed in claim 7.

11. A communication system comprising at least a pair of computing entities as claimed in claim 10 and a communications medium, each of said pair of computing entities being arranged to communicate with the other computing entity via the communications medium.

12. A communication system as claimed in claim 11 in which said communications medium includes one or more of any of the internet, local area network, wide area network, virtual private circuit or public telecommunications network.

13. A computer storage medium having stored thereon a computer program readable by a general purpose computer, the computer program including instructions for said general purpose computer to configure it to be as said computer entity as claimed in claim 4 or said computer entity as claimed in claim 7.

14. A method of exchanging digital public-key verification data, a computing entity, a communications system, a system of cooperating computing entities or a computer storage medium substantially as hereinbefore described with reference to the accompanying drawings.

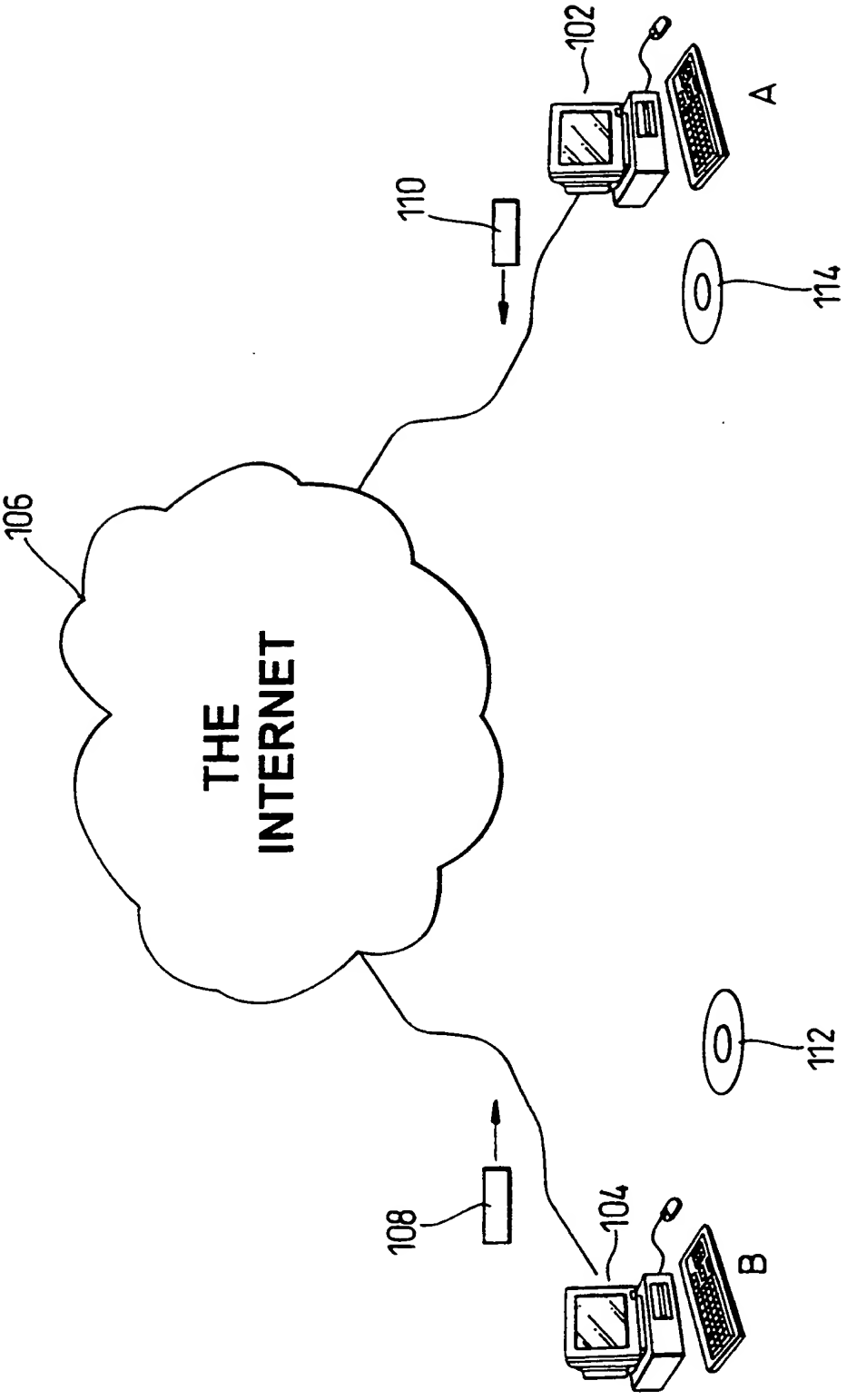


Fig. 1

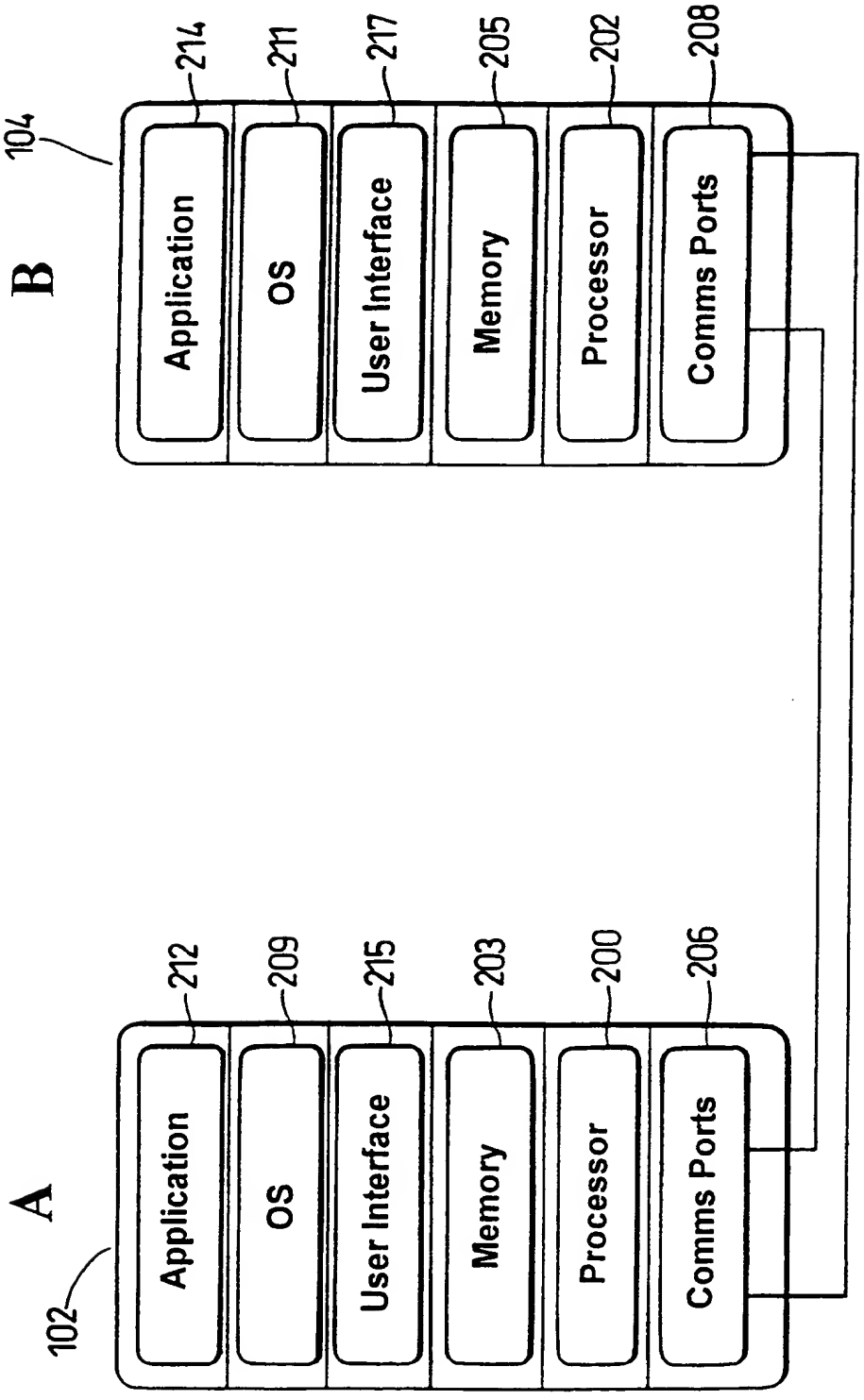

B
104
214
211
217
205
202
208
Application
OS
User Interface
Memory
Processor
Comms Ports
A
102
212
209
215
203
200
206
Application
OS
User Interface
Memory
Processor
Comms Ports

Fig. 2

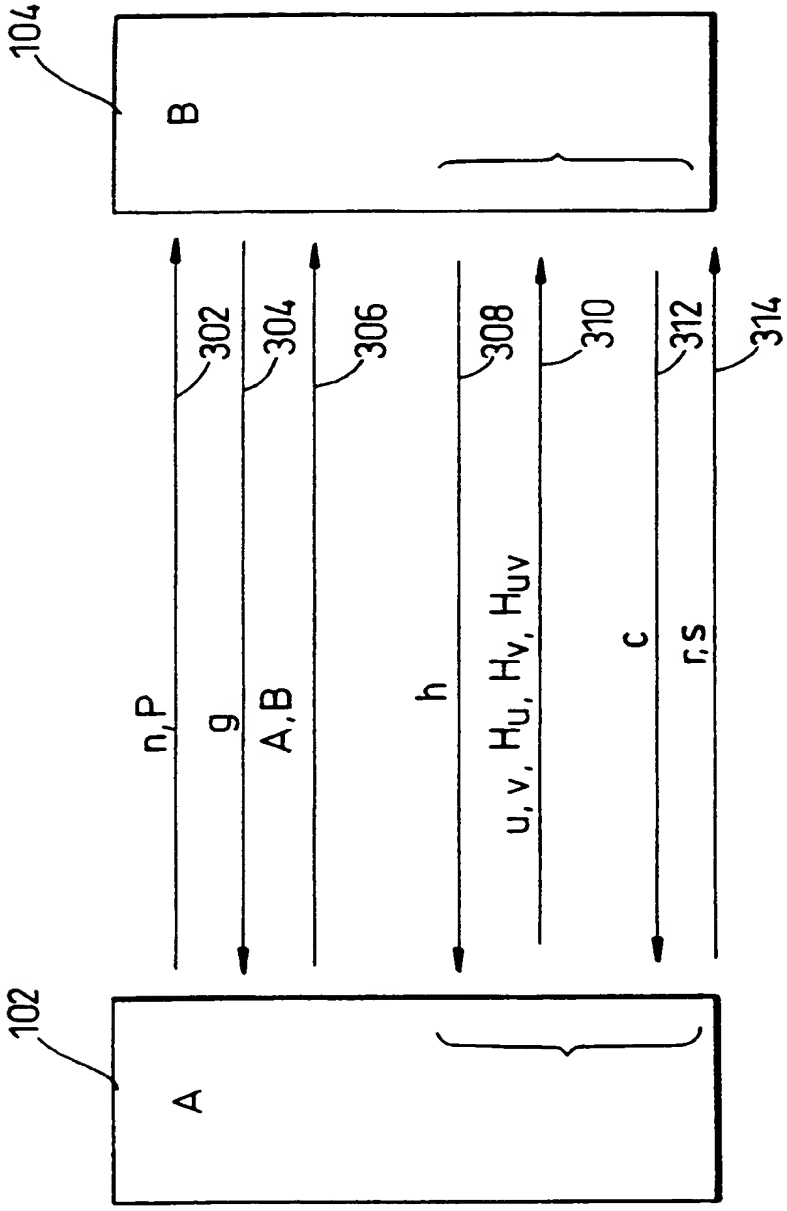


Fig. 3

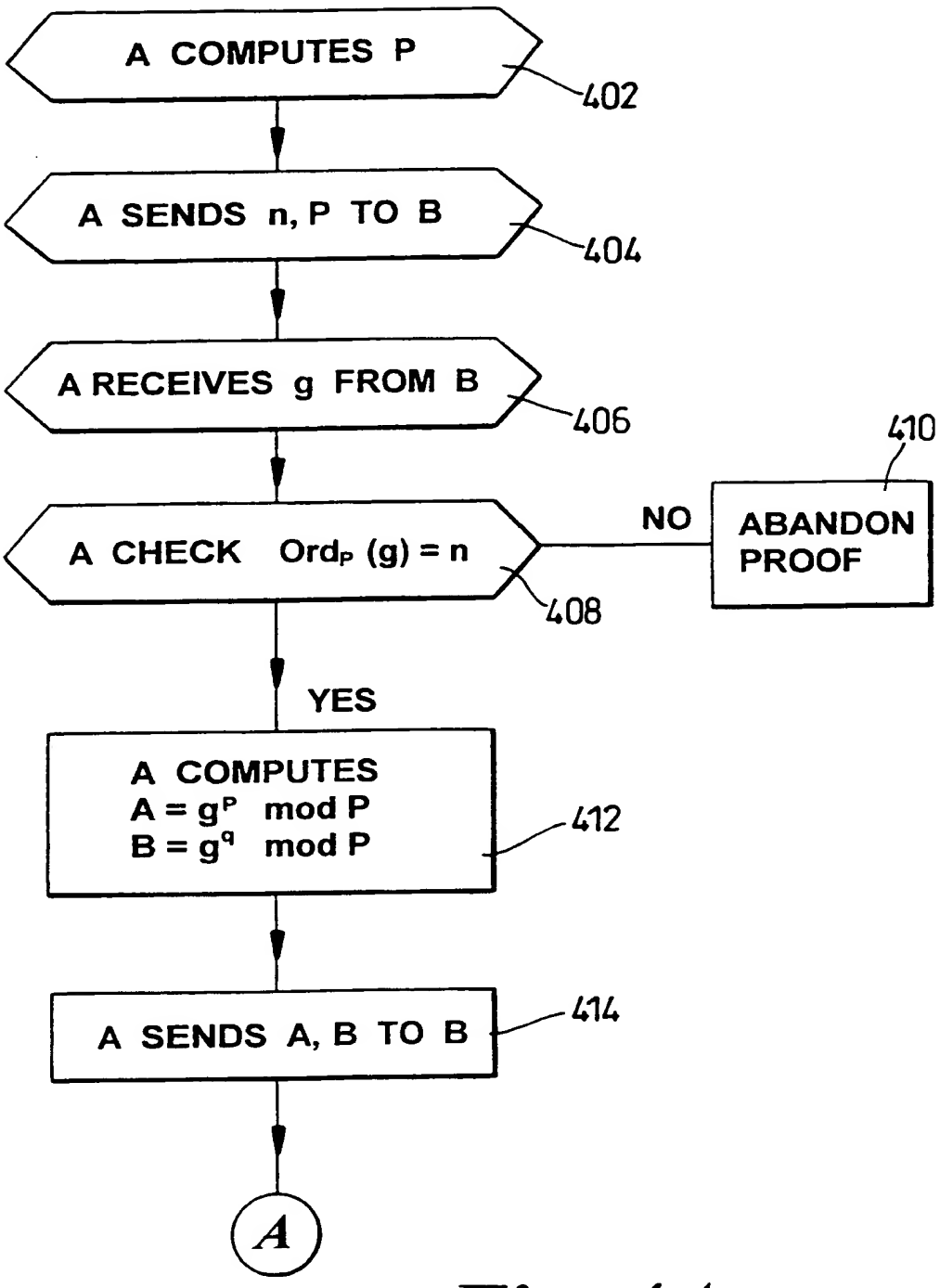

A COMPUTES P
402
A SENDS n, P TO B
404
A RECEIVES g FROM B
406
410
NO
ABANDON PROOF
A CHECK Ord$_P$ (g) = n
408
YES
A COMPUTES
A = g^P mod P
B = g^q mod P
412
A SENDS A, B TO B
414
A

Fig. 4A

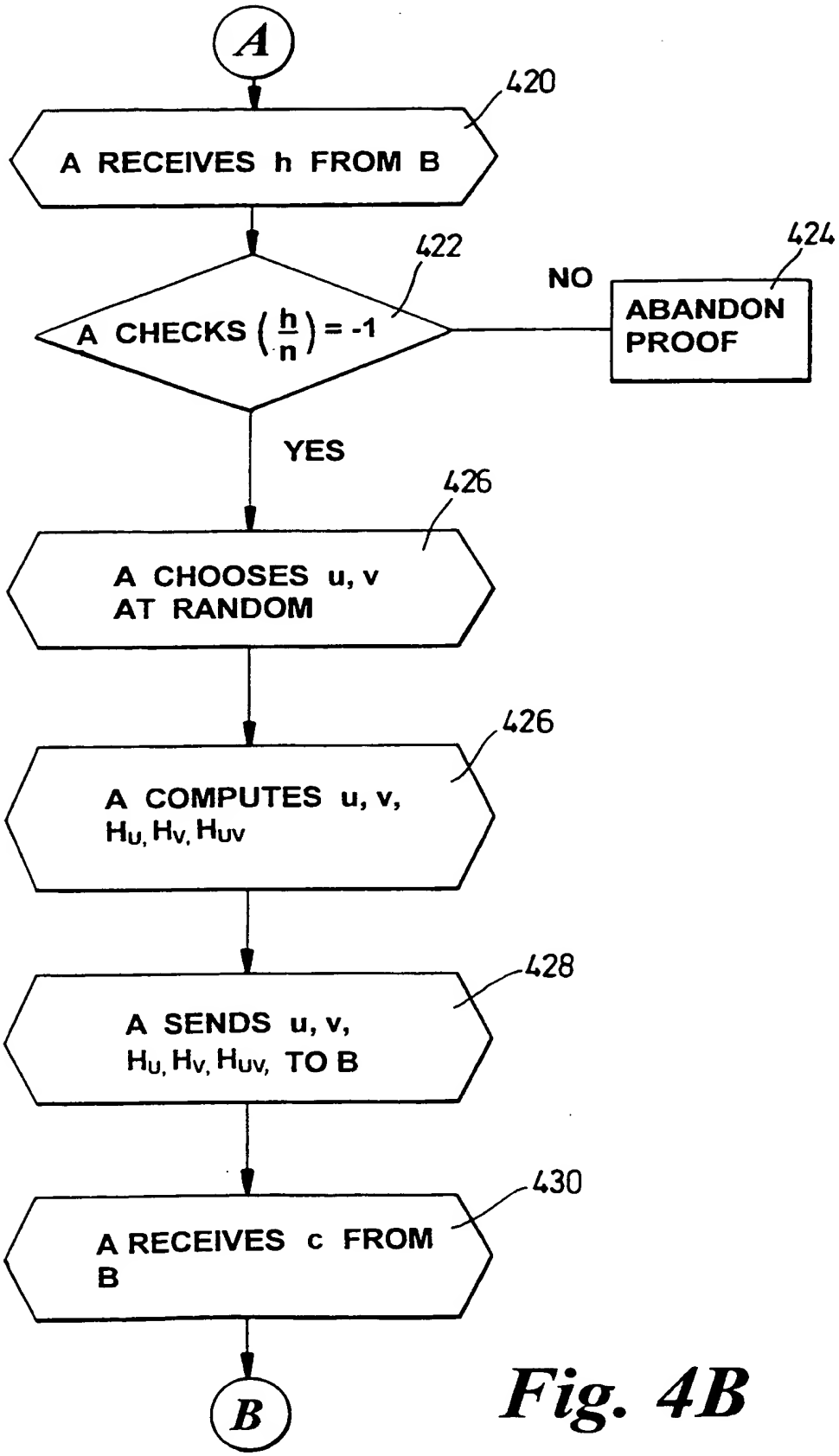

A
420
A RECEIVES h FROM B
422
A CHECKS $\left(\frac{h}{n}\right) = -1$
NO
424
ABANDON PROOF
YES
426
A CHOOSES u, v AT RANDOM
426
A COMPUTES u, v, H_U, H_V, H_{UV}
428
A SENDS u, v, H_U, H_V, H_{UV}, TO B
430
A RECEIVES c FROM B
B

Fig. 4B

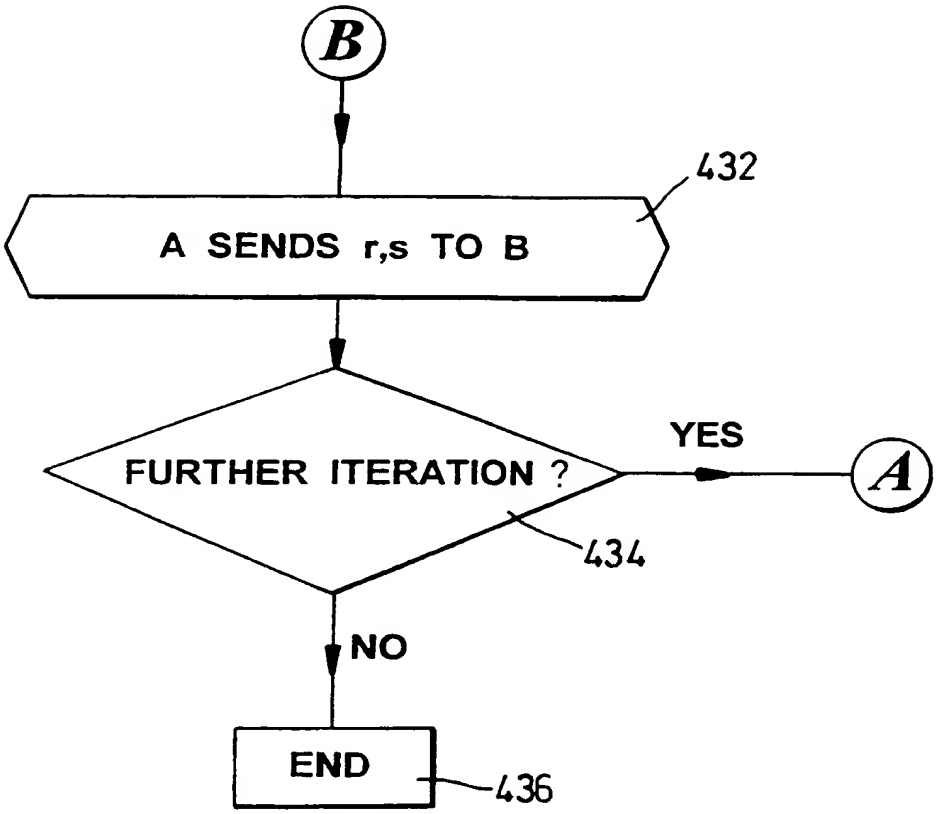


Fig. 4C

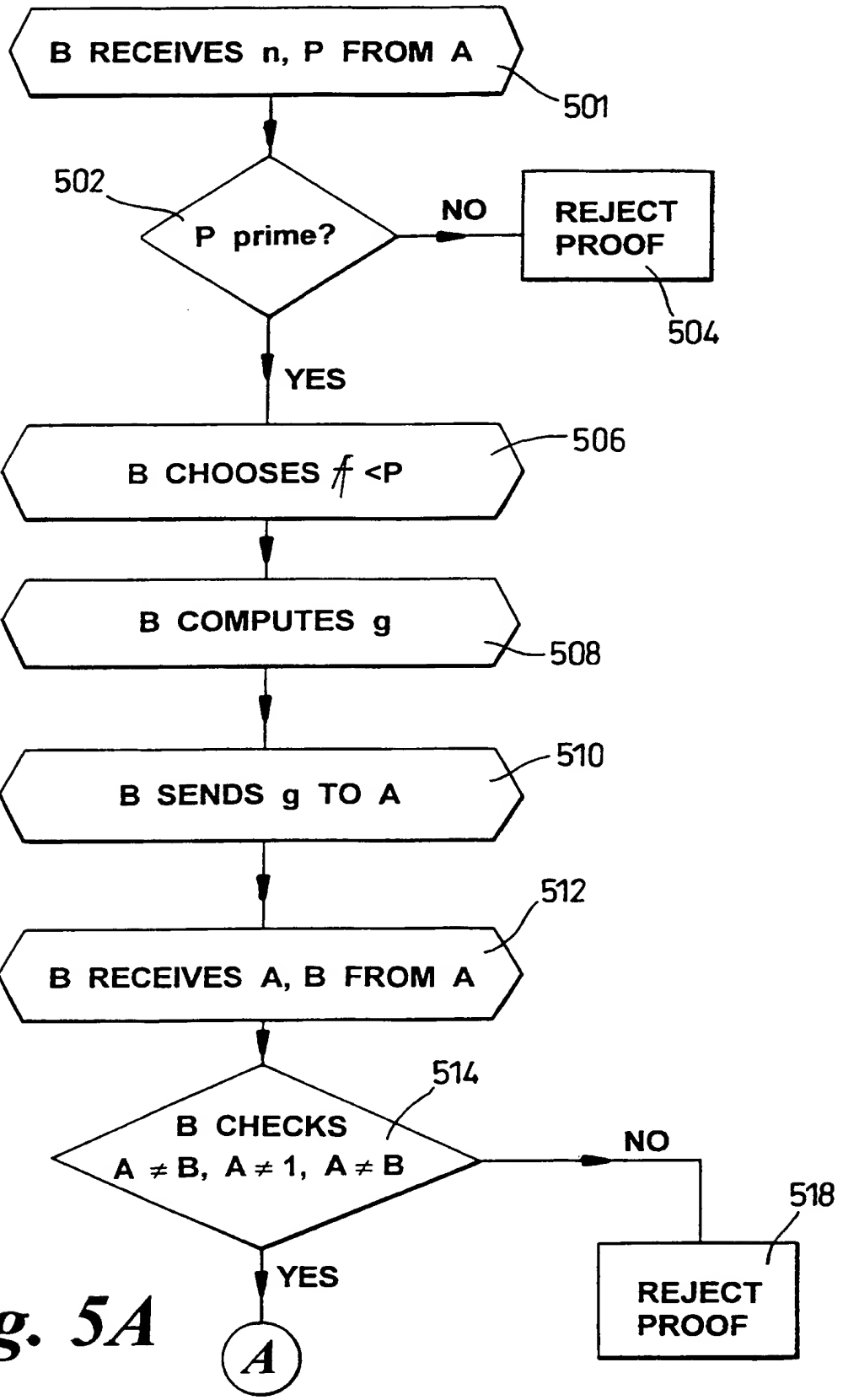

B RECEIVES n, P FROM A
501
502
P prime?
NO
REJECT PROOF
504
YES
B CHOOSES f <P
506
B COMPUTES g
508
B SENDS g TO A
510
B RECEIVES A, B FROM A
512
B CHECKS
A ≠ B, A ≠ 1, A ≠ B
514
NO
518
REJECT PROOF
YES
A

Fig. 5A

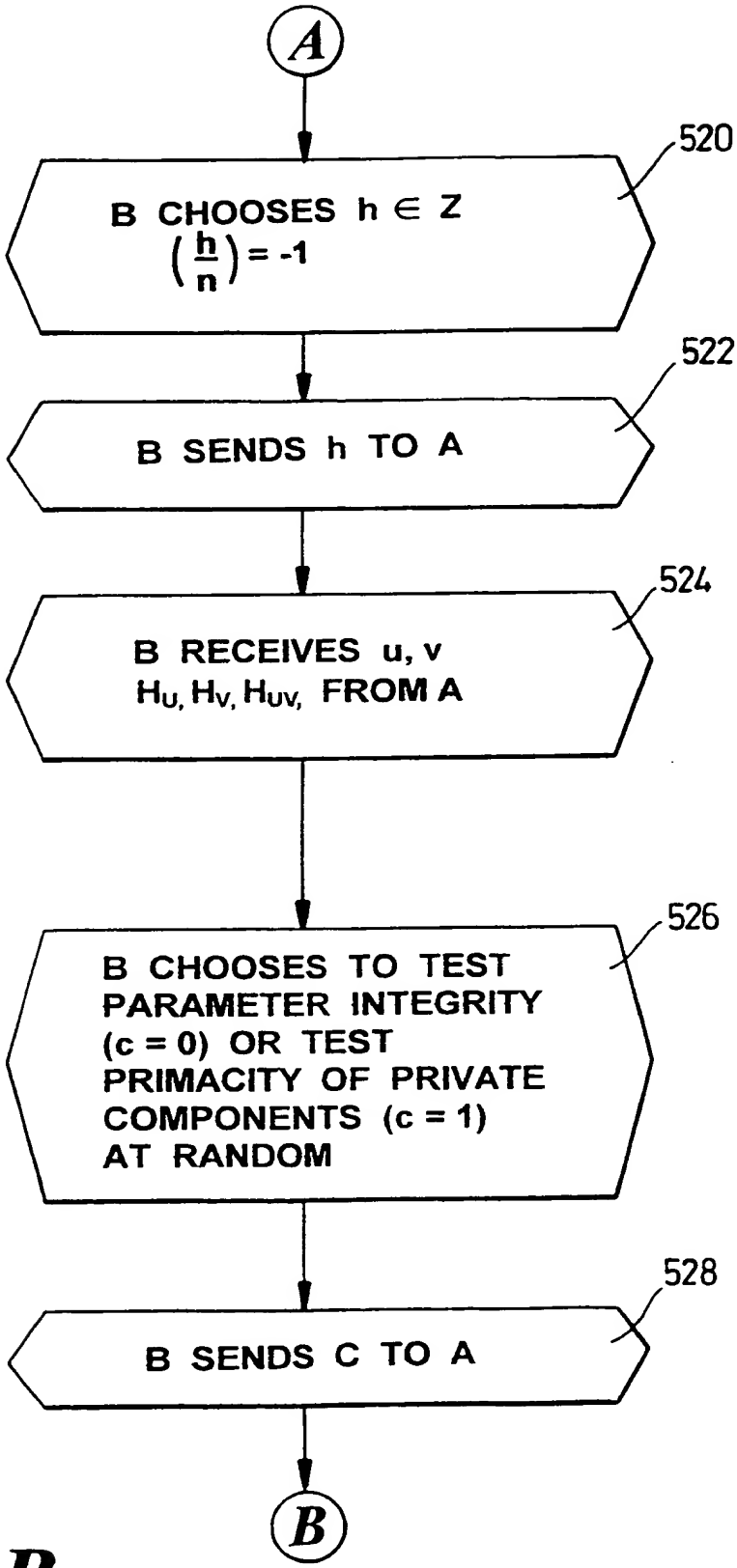

A
520
B CHOOSES h ∈ Z
(h/n) = -1
522
B SENDS h TO A
524
B RECEIVES u, v
Hu, Hv, Huv, FROM A
526
B CHOOSES TO TEST
PARAMETER INTEGRITY
(c = 0) OR TEST
PRIMACITY OF PRIVATE
COMPONENTS (c = 1)
AT RANDOM
528
B SENDS C TO A
B

Fig. 5B

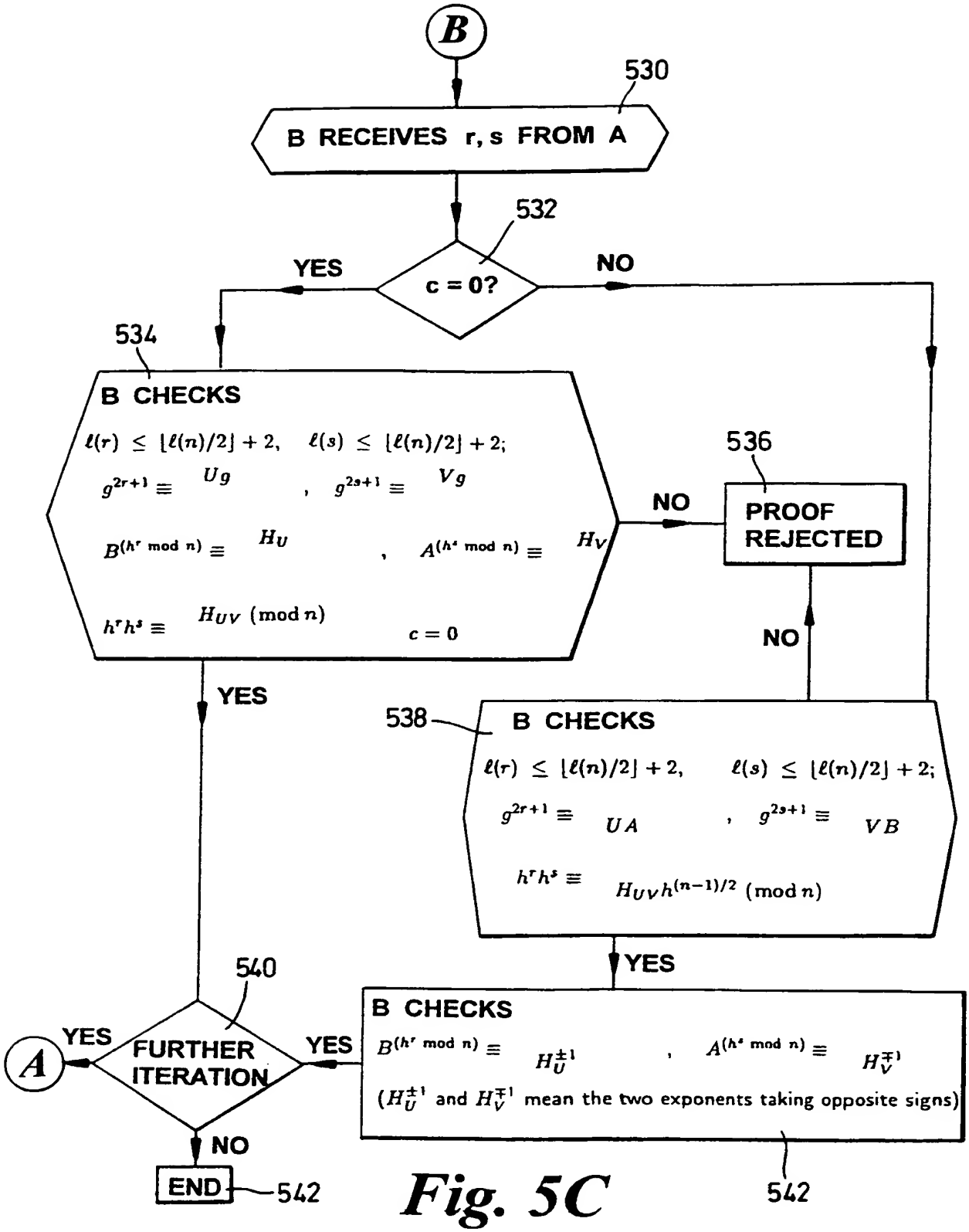

B
530
B RECEIVES r, s FROM A
532
c = 0?
YES
NO
534
B CHECKS
$\ell(r) \leq \lfloor \ell(n)/2 \rfloor + 2, \quad \ell(s) \leq \lfloor \ell(n)/2 \rfloor + 2;$
$g^{2r+1} \equiv Ug$, $g^{2s+1} \equiv Vg$
$B^{(h^r \bmod n)} \equiv H_U$, $A^{(h^s \bmod n)} \equiv H_V$
$h^r h^s \equiv H_{UV} \pmod n$
$c = 0$
536
NO
PROOF REJECTED
NO
YES
538
B CHECKS
$\ell(r) \leq \lfloor \ell(n)/2 \rfloor + 2, \quad \ell(s) \leq \lfloor \ell(n)/2 \rfloor + 2;$
$g^{2r+1} \equiv UA$, $g^{2s+1} \equiv VB$
$h^r h^s \equiv H_{UV} h^{(n-1)/2} \pmod n$
YES
540
A
YES
FURTHER ITERATION
YES
B CHECKS
$B^{(h^r \bmod n)} \equiv H_U^{\pm 1}$, $A^{(h^s \bmod n)} \equiv H_V^{\mp 1}$
($H_U^{\pm 1}$ and $H_V^{\mp 1}$ mean the two exponents taking opposite signs)
NO
END
542
542

Fig. 5C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 00/00370

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	R. BERGER, S. KANNAN, R. PERALTA: "A Framework for the Study of Cryptographic Protocols" ADVANCES IN CRYPTOLOGY - PROCEEDINGS OF CRYPTO 85, 18 - 22 August 1985, pages 87-103, XP002136911 cited in the application	1-14
A	BLUM M: "Coin flipping by telephone-a protocol for solving impossible problems" DIGEST OF PAPERS SPRING COMPCON 82. HIGH TECHNOLOGY IN THE INFORMATION INDUSTRY, SAN FRANCISCO, CA, USA, 22-25 FEB. 1982, pages 133-137, XP000892068 1982, New York, NY, USA, IEEE, USA cited in the application page 135 -page 136	1,4,7,13

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 May 2000	19/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Zucka, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	GOLDWASSER S: "Multi-party computations: past and present" PROCEEDINGS OF THE SIXTEENTH ANNUAL ACM SYMPOSIUM ON PRINCIPLES OF DISTRIBUTED COMPUTING, PROCEEDINGS OF PODC 97: 16TH ACM SYMPOSIUM ON PRINCIPLES OF DISTRIBUTED COMPUTING, SANTA BARBARA, CA, USA, 21-24 AUG. 1997, pages 1-6, XP000892069 1997, New York, NY, USA, ACM, USA ISBN: 0-89791-952-1 page 2 -page 4	1,4,7,13